kaspersky

Kaspersky Security Center Cloud Console

Índice

Chave ativa

Chave de acesso AWS IAM

Chave de assinatura adicional

Configurações de Programa

Configurações de tarefa

Console de Gerenciamento AWS

Conta no Kaspersky Security Center Cloud Console

Dispositivo de proteção UEFI

Dispositivo gerenciado

Domínio de difusão

Espaço de trabalho

Função do IAM

Gateway de conexão

Gerenciamento centralizado de aplicativos

Gerenciamento de identidades e acesso (IAM)

Gerenciamento direto de aplicativos

Gravidade do evento

Grupo de administração

HTTPS

Identificador do aplicativo

Imagem de máquina da Amazon (AMI, Amazon Machine Image)

Instalação forçada

Instalação local

Instalação remota

Instância Amazon EC2

Interface do Programa de Aplicativo AWS (AWS API)

JavaScript

Kaspersky Private Security Network (KPSN)

Kaspersky Security Network (KSN)

Limite de atividade de vírus

Nível de importância do patch

Operador do Kaspersky Security Center Cloud Console

Pacote de instalação

Perfil da política

Período da licença

Plug-in da Web de gerenciamento

Política

Ponto de distribuição

Proprietário do dispositivo

Proteção antivírus da rede

Quarentena

Repositório de eventos

Restauração

Servidor de Administração

Servidor de Administração Principal

Servidor de Administração virtual

Servidores de atualização da Kaspersky

SSL

Ajuda do Kaspersky Security Center Cloud Console

O que há de novo

Descubra o que há de novo na versão mais recente do aplicativo.

Configuração da proteção da rede

Gerencie a segurança de uma organização configurando as políticas e tarefas do aplicativo Kaspersky de acordo com os requisitos da organização.

Requisitos de hardware e software

Verifique quais sistemas operacionais e versões de aplicativo são compatíveis.

Aplicativos Kaspersky: atualizando periódica dos bancos de dados e módulos de software

Mantenha a confiabilidade do sistema de proteção.

Licenciamento do Kaspersky Security Center Cloud Console

Saiba mais sobre o funcionamento do Kaspersky Security Center Cloud Console em modo de avaliação e no modo comercial.

Monitoramento e relatórios

Visualize sua infraestrutura, os status da proteção de dispositivos em rede e estatísticas para gerenciar o estado atual da proteção de sua organização. Você também pode usar relatórios.

Configuração inicial

Ao começar a trabalhar com seu espaço de trabalho, configure o Kaspersky Security Center Cloud Console de acordo com suas necessidades.

Gerenciamento de patches e vulnerabilidades

Encontre e corrija vulnerabilidades em softwares de terceiros.

Migração para o Kaspersky Security Center Cloud Console

Migre os grupos de administração existentes e os objetos relacionados do Kaspersky Security Center do local para o Kaspersky Security Center Cloud Console.

Exportando eventos para os sistemas SIEM

Configure a exportação de eventos para sistemas SIEM usando o protocolo Syslog.

Localizar dispositivos na rede

Descubra os dispositivos existentes e os novos na rede da sua organização.

Trabalhando em um ambiente nuvem

Proteja as máquinas virtuais em ambientes em nuvem: Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.

Ajustar pontos de distribuição e/ou gateways de conexão

Configurar os pontos de distribuição.

Manual de Início Rápido para Provedores de Serviços Gerenciados (MSPs)

Aprenda a trabalhar com o Kaspersky Security Center Cloud Console se for um administrador do MSP.

Aplicativos Kaspersky: implementação centralizada

Implementar aplicativos Kaspersky.

O que há de novo

Atualização de abril de 2024

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- Um novo recurso do Cloud Discovery. Esse recurso permite monitorar o uso de serviços em nuvem em dispositivos gerenciados que executam o Windows e bloquear o acesso a serviços em nuvem que considerar indesejados. A Cloud Discovery rastreia as tentativas do usuário de obter acesso a esses serviços por meio de navegadores e aplicativos desktop.

Atualização de fevereiro de 2024

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- Na lista de dispositivos gerenciados, agora é possível selecionar um ou vários dispositivos e atribuir uma tarefa existente para ser executada nos dispositivos selecionados. O escopo do dispositivo atual da tarefa será substituído pelos dispositivos selecionados.

- Agora é possível atribuir tags de dispositivo a vários dispositivos ou remover tags de dispositivo de vários dispositivos de uma só vez. Na lista de dispositivos gerenciados, selecione os dispositivos e especifique quais tags você deseja atribuir ou remover dos respectivos dispositivos.

- Aparência otimizada e experiência do usuário da lista de dispositivos gerenciados. Adicionada a nova coluna **Tags** e a capacidade de filtrar dispositivos por tags de dispositivo.

Atualização de janeiro de 2024

O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Endpoint Security 12.4 for Windows.

Atualização de dezembro de 2023

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- Agora é possível verificar a conexão com um sistema SIEM.

- O Kaspersky Security Center Cloud Console agora é compatível com a sondagem de um controlador de domínio do Microsoft Active Directory e um controlador de domínio Samba por meio de um ponto de distribuição baseado em Linux.

- Diagnóstico remoto de dispositivos gerenciados baseados em Linux.

- O Kaspersky Security Center Cloud Console agora oferece suporte ao seguintes aplicativos da Kaspersky:

  - Kaspersky Endpoint Security for Windows versão 12.3 Patch A

  - Kaspersky Endpoint Security 12.0 for Linux

  - Kaspersky Endpoint Security 12.0 for Mac

- Kaspersky Endpoint Agent 3.16
- Kaspersky Embedded Systems Security 3.3 for Windows

- Duas seções da interface foram ocultadas no menu principal como fora do escopo da funcionalidade do aplicativo:
  - Eventos de criptografia (**Operações → Criptografia e proteção de dados → Eventos de criptografia**)
  - Intervalos de IPs (**Descoberta e implementação → Descoberta → Intervalos de IPs**)
- Atualizamos o texto do Acordo de Processamento de Dados do Kaspersky Security Center Cloud Console.
- Várias versões antigas do navegador não são mais compatíveis (Firefox ESR anterior à versão 102).

Atualização de setembro de 2023

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Embedded Systems Security 3.3 for Linux.
- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Endpoint Security 12.2 for Windows.
- Otimização da interface do usuário ao trabalhar com a lista de usuários na seção **Ativos (dispositivos)**.

Atualização de junho de 2023

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- Um novo Guia de Proteção foi lançado. É altamente recomendável ler atentamente o guia e seguir as recomendações de segurança para configurar o Kaspersky Security Center Cloud Console e sua infraestrutura de rede.
- Agora, o Kaspersky Security Center Cloud Console é compatível com o Kaspersky Endpoint Security 11.3 for Mac.
- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Endpoint Security 11.4 for Linux.
- É possível usar o Kaspersky Security Center Cloud Console para exportar seleções de eventos para um arquivo e, em seguida, importar as seleções de evento para o Kaspersky Security Center Windows ou Kaspersky Security Center Linux.
- Agora, é possível usar um ponto de distribuição como um servidor push para os dispositivos gerenciados pelo Agente de Rede. Esse recurso permite garantir que conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração seja estabelecida.
- Reorganização da seção com configurações para integrar o Kaspersky Security Center Cloud Console com outros aplicativos da Kaspersky.
- Reorganização da interface do usuário da seção **Diagnóstico remoto**.

- Agora, é possível salvar as informações sobre todos os dispositivos incluídos em uma seleção de dispositivos em um arquivo CSV de uma só vez.

- Uma série de melhorias na interface do usuário e na usabilidade, incluindo a capacidade de selecionar todos os itens em uma tabela.

Atualização de março de 2023

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- O Kaspersky Security Center Cloud Console agora oferece suporte a clusters e matrizes de servidores como dispositivos gerenciados. Se um aplicativo Kaspersky estiver instalado em um nó de cluster, o Agente de Rede envia essas informações para o Servidor de Administração. No Web Console, clusters e matrizes de servidores são listados separadamente de outros dispositivos gerenciados. Você gerencia cada cluster ou matriz de servidor como um objeto individual e inseparável.

- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Endpoint Security 12.0 for Windows.

- O número máximo de entradas que um relatório pode incluir foi aumentado para 2.500 para um relatório no Web Console e até 10.000 para um relatório exportado para um arquivo.

- Agora é possível escolher se deseja ou não incluir os dispositivos gerenciados com o status *OK* no relatório de status da proteção.

- Agora é possível ativar o Kaspersky Security Center Cloud Console usando uma das seguintes licenças ou adicionar as chaves de licença das licenças listadas para um espaço de trabalho existente:

  - Kaspersky Symphony Security

  - Kaspersky Symphony EDR

  - Kaspersky Symphony MDR

  - Kaspersky Symphony XDR

- Uma edição especial de Agente de Rede para Windows XP foi liberada.

- O Agente de Rede atualizado para Linux suporta o Serviço de proxy da KSN. Juntamente com os pontos de distribuição baseados em Windows, agora é possível usar pontos de distribuição baseados em Linux para encaminhar solicitações da Kaspersky Security Network (KSN) dos dispositivos gerenciados. Esse recurso permite redistribuir e otimizar o tráfego na rede.

- O Agente de Rede para Linux atualizado é compatível com o recurso de registro de aplicativos. O Agente de Rede pode compilar uma lista de aplicativos instalados em um dispositivo gerenciado baseado em Linux e, a seguir, transmite esta lista para o Servidor de Administração.

- É possível usar o Kaspersky Security Center Cloud Console para exportar políticas e tarefas para um arquivo e, em seguida, importar as políticas e as tarefas para o Kaspersky Security Center Windows ou Kaspersky Security Center Linux.

Atualização de novembro de 2022

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Endpoint Security 11.3 for Linux.
- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Managed Detection and Response Optimum 2.1.18.
- O Kaspersky Security Center Cloud Console agora oferece suporte para as versões atualizadas do Kaspersky Endpoint Security for Mac 11.2 e 11.2.1 para garantir a compatibilidade com o macOS 13.
- Os vídeos na seção **Introdução e tutoriais** foram atualizados.

Atualização de outubro de 2022

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- Atualizamos o texto do Acordo de Processamento de Dados do Kaspersky Security Center Cloud Console.
- A infraestrutura do Kaspersky Security Center Cloud Console agora notifica você de espaços de trabalho que não tenham chave de licença ativa e que poderão ser excluídos se você não adicionar uma nova chave de licença.
- Agora, o Kaspersky Security Center Cloud Console é compatível com o Kaspersky Endpoint Security 11.11.0 for Windows.
- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Endpoint Detection and Response Optimum 2.3.
- O Kaspersky Embedded Systems Security 3.2 for Windows é compatível.

Atualização de setembro de 2022

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- Agora é possível atribuir administradores dedicados para Servidores de Administração virtuais. Você cria uma conta de usuário para um administrador e, em seguida, concede a ele os direitos de acesso a um Servidor de Administração virtual. O administrador atribuído tem acesso apenas ao Servidor de Administração virtual selecionado e não pode se conectar ao Servidor de Administração principal ou a outros Servidores de Administração secundários, físicos ou virtuais.
- Experiência do usuário otimizada ao excluir uma chave de licença do Kaspersky Security Center Cloud Console. O novo mecanismo impede que você exclua sua última chave de licença ativa por acidente.
- Agora, é possível usar pontos de distribuição baseados em Linux para baixar bancos de dados antivírus para aplicativos de segurança da Kaspersky com a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*.
- Agora, o Agente de Rede está disponível na localização em japonês.
- Na interface do Kaspersky Security Center Cloud Console, o estilo todo em maiúsculas dos nomes das seções foi alterado para o uso de maiúsculas em estilo de frase.

Atualização de agosto de 2022

Suporte a novo idioma: o Kaspersky Security Center Cloud Console está totalmente disponível no idioma japonês.

Atualização de julho de 2022

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- Novas versões de aplicativos da Kaspersky compatíveis:
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 for Mac
  - Kaspersky Security for iOS 1.0.0
  - Kaspersky Endpoint Security 11.10.0 for Windows
- Atualizamos o texto do Contrato e do Acordo de Processamento de Dados do Kaspersky Security Center Cloud Console.
- Suporte a novo idioma: a infraestrutura do Kaspersky Security Center Cloud Console agora está disponível em japonês. Em breve, será disponibilizado o idioma japonês nos espaços de trabalho do Kaspersky Security Center Cloud Console.

Atualização de abril de 2022

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Endpoint Security 11.9.0 for Windows.
- O Kaspersky Security Center Cloud Console agora oferece suporte à localização em japonês do Kaspersky Embedded Systems Security.

Atualização de 9 de março de 2022

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- A Integração com o Kaspersky Endpoint Detection and Response Expert é implementada.
- A Incident Response Platform (IRP) é implementada. Agora é possível gerenciar incidentes de segurança por meio do Kaspersky Security Center Cloud Console.
- O Kaspersky Security Center Cloud Console agora aceita chaves de licença para o Kaspersky Endpoint Detection and Response Expert. O número mínimo de dispositivos para a licença é 50.

Atualização de 11 de fevereiro de 2022

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- Licenças para O Kaspersky Embedded Systems Security for Windows agora são compatíveis.

- O Kaspersky Endpoint Security 11.8.0 for Windows é compatível.
- É possível instalar o Kaspersky Endpoint Security 11.8.0 for Windows usando um pacote de distribuição em japonês.
- O Kaspersky Endpoint Agent 3.12 é compatível.

Atualização em 10 de dezembro de 2021

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- O trabalho com usuários internos foi aprimorado:
  - Agora você pode adicionar novos usuários internos no portal.
  - O aplicativo agora impede que você diminua seus próprios direitos.

Atualização de 18 de outubro de 2021

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Endpoint Detection and Response Optimum 2.0.
- Agora, você pode gerenciar dispositivos móveis executados em Android usando o Kaspersky Security Center Cloud Console.
- O Kaspersky Marketplace está disponível como uma nova seção de menu: você pode pesquisar aplicativos Kaspersky usando o Kaspersky Security Center Cloud Console.
- Esta disponível uma nova seção de menu, Novidades Kaspersky. As Novidades Kaspersky mantém você a par de informações relacionadas aos aplicativos Kaspersky instalados nos dispositivos gerenciados. O Kaspersky Security Center Cloud Console atualiza periodicamente as informações da seção.
- Agora você pode gerenciar Servidores de Administração secundários em execução em sistemas operacionais Linux, por meio do Kaspersky Security Center Cloud Console.

Atualização de 7 de setembro de 2021

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- Agora você pode usar os Serviços de Federação do Active Directory (ADFS) para fazer login no Kaspersky Security Center Cloud Console usando sua conta do Active Directory, sem criar uma nova conta de usuário.
- O Kaspersky Security Center Cloud Console agora funciona com os seguintes ambientes de nuvem: Amazon Web Services, Microsoft Azure e Google Cloud. Para proteger máquinas virtuais (ou instâncias) em um ambiente de nuvem, você precisa de uma das Licenças do Kaspersky Hybrid Cloud Security. O Assistente de configuração de ambiente em nuvem está disponível.
- A quantidade máxima de dispositivos por cada espaço de trabalho é agora 25.000.
- A integração com os sistemas SIEM agora está disponível no Kaspersky Security Center Cloud Console. Você pode exportar eventos para sistemas SIEM usando o protocolo Syslog.

- Agora você pode criar servidores de administração virtuais. Cada Servidor de Administração virtual pode ter sua própria estrutura de grupos de administração, políticas, tarefas, relatórios e eventos. Você pode usar servidores de administração virtuais para o gerenciamento de organizações clientes com fluxos de trabalho complicados em sua área de trabalho. No entanto, você não pode migrar os Servidores de Administração virtuais do Kaspersky Security Center em execução local para o Kaspersky Security Center Cloud Console.
- Agora você pode ajustar a largura das colunas nas tabelas, classificar e pesquisar dados.
- Aprimoramos a estabilidade e a disponibilidade do Kaspersky Business Hub e do Kaspersky Security Center Cloud Console.

Atualização de 27 de outubro de 2020

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- Agora, o Kaspersky Security Center Cloud Console é compatível com o Kaspersky Endpoint Security 11.6.0 for Windows, Kaspersky Endpoint Security 11.1 for Mac Patch A e Kaspersky Endpoint Agent 3.10 (como parte do Kaspersky Endpoint Detection and Response Optimum).
- As seguintes licenças podem ser usadas:
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Endpoint Security for Business Advanced
  - Kaspersky Total Security for Business
- Os seguintes recursos são implementados:
  - Gerenciamento de Patches e Vulnerabilidades
  - Gerenciamento de criptografia
  - Controle de Aplicativos
  - Controle Adaptativo de Anomalias
  - Sessões RDP, incluindo Compartilhamento da área de trabalho do Windows
- O menu de navegação agora é vertical, semelhante à interface baseada no Microsoft Management Console do Kaspersky Security Center.
- Vídeos de treinamento técnico já estão disponíveis e ajudarão você a aprender como o aplicativo funciona.

Atualização de 30 de junho de 2020

Esta atualização do Kaspersky Security Center Cloud Console inclui os seguintes novos recursos e melhorias:

- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Security 11 for Windows Server (a partir de setembro de 2020).
- O Kaspersky Security Center Cloud Console agora é compatível com o Kaspersky Endpoint Agent 3.9 e o Kaspersky Endpoint Security 11.4.0 for Windows.

- O Assistente de Início Rápido foi aprimorado: algumas etapas foram removidas, a sequência de etapas foi ligeiramente alterada e alguns textos foram editados para facilitar o uso.

- O Kaspersky Security Center Cloud Console agora está disponível no idioma italiano.

- Agora você pode revogar o EULA (Contrato de Licença do Usuário Final) de qualquer aplicativo Kaspersky gerenciado por meio da interface do Kaspersky Security Center Cloud Console. É necessário desinstalar o aplicativo selecionado antes de revogar seu EULA.

- Agora você pode excluir áreas de trabalho. Se você marcar um espaço de trabalho para exclusão, por padrão, ele será excluído automaticamente em sete dias. No entanto, é possível forçar a exclusão do espaço de trabalho para que ele seja excluído imediatamente.

- A verificação em duas etapas para acessar o console foi implementada.

Kaspersky Security Center Cloud Console

A seção contém informações sobre a finalidade do Kaspersky Security Center Cloud Console, assim como os respectivos recursos e componentes principais.

O Kaspersky Security Center Cloud Console é um aplicativo hospedado e mantido pela Kaspersky. Não é necessário instalar o Kaspersky Security Center Cloud Console em seu computador ou servidor. O Kaspersky Security Center Cloud Console permite que o administrador instale aplicativos de segurança da Kaspersky em dispositivos em uma rede corporativa, execute remotamente tarefas de verificação e atualização e gerencie as políticas de segurança dos aplicativos gerenciados. O administrador pode usar um painel detalhado que fornece uma visão instantânea do status de dispositivos corporativos, relatórios detalhados e configurações granulares nas políticas de proteção.

Sobre o Kaspersky Security Center Cloud Console

O Kaspersky Security Center Cloud Console é um aplicativo que se destina aos administradores de redes corporativas e funcionários responsáveis pela proteção de dispositivos em diversos tipos de organizações.

O Kaspersky Security Center Cloud Console permite que você faça o seguinte:

- Instalar aplicativos da Kaspersky em dispositivos em sua rede e gerenciar os aplicativos instalados.
- Crie uma hierarquia de grupos de administração para gerenciar uma seleção de dispositivos cliente como um todo.
- Crie Servidores de Administração virtuais e organize-os hierarquicamente.
- Proteja seus dispositivos de rede, incluindo estações de trabalho e servidores:
  - Gerencie um sistema de proteção antimalware integrado aos aplicativos Kaspersky.
  - Use os recursos de detecção e resposta (EDR e MDR) (é necessária uma licença para o Kaspersky Endpoint Detection and Response e/ou para Kaspersky Managed Detection and Response), incluindo:
    - Análise e investigação de incidentes
    - Visualização de incidentes por meio da criação de um gráfico da cadeia de desenvolvimento de ameaças
    - Aceite ou recusa manual de respostas ou configuração de aceitação automática de todas as respostas
- Use o Kaspersky Security Center Cloud Console como um aplicativo multi-tenant.
- Gerencie remotamente os aplicativos da Kaspersky instalados nos dispositivos clientes.
- Realize a implementação centralizada de chaves de licença para aplicativos da Kaspersky nos dispositivos cliente.
- Crie e gerencie políticas de segurança para dispositivos em sua rede.
- Crie e gerencie contas de usuário.
- Crie e gerencie funções de usuário (RBAC).

- Crie e gerencie tarefas para aplicativos instalados em dispositivos na rede.
- Visualize relatórios sobre o status do sistema de segurança para cada organização cliente individualmente.

Você gerencia o Kaspersky Security Center Cloud Console usando um Console de Administração baseado na nuvem que garante a interação entre o seu dispositivo e o Servidor de Administração através de um navegador. O Servidor de Administração é um aplicativo projetado para gerenciar aplicativos da Kaspersky instalados nos dispositivos na sua rede. Quando você se conecta ao Kaspersky Security Center Cloud Console usando seu navegador, o navegador estabelece uma conexão com o Kaspersky Security Center Cloud Console.

O Servidor de Administração e o DBMS (Sistema de Gerenciamento de Banco de Dados) conectado são implantados em um ambiente em nuvem e fornecidos a você como um serviço. A manutenção do servidor de administração e do DBMS foi incluída como parte do serviço. Todos os componentes de software do Kaspersky Security Center Cloud Console são mantidos atualizados. É feito o backup regular do Servidor de Administração e dos objetos criados (como políticas e tarefas) para mantê-los seguros.

O Kaspersky Security Center Cloud Console é um aplicativo disponível em vários idiomas. Você pode alterar o idioma da interface a qualquer momento, sem necessidade de reabrir o aplicativo.

Requisitos de hardware e software para o Kaspersky Security Center Cloud Console

Console de Administração

Em um cliente, o uso do Kaspersky Security Center Cloud Console somente requer um navegador.

> Somente é possível usar uma única janela ou guia do navegador para trabalhar com o Kaspersky Security Center Cloud Console.

Os requisitos de hardware e software para o dispositivo são idênticos aos requisitos do navegador utilizado com o Kaspersky Security Center Cloud Console.

Navegador:

- Google Chrome 100.0.4896.88 ou posterior (compilação oficial)
- Microsoft Edge 100 ou posterior
- Safari 15 no macOS
- Navegador "Yandex" 23.5.0.2271
- Mozilla Firefox Extended Support Release 102.0 ou posterior

Agente de Rede

Requisitos mínimos de hardware:

- CPU com frequência operacional de 1 GHz ou superior. Para um SO de 64 bits, a frequência mínima de CPU é de 1.4 GHz.

- RAM: 512 MB.
- Espaço disponível em disco: 1 GB.

Requisitos mínimos de hardware para Gerenciamento de vulnerabilidades e patches:

- CPU com frequência operacional de 1.4 GHz ou superior. É necessário um sistema operacional de 64 bits.
- RAM: 8 GB.
- Espaço disponível em disco: 1 GB.

Sistemas operacionais compatíveis com o Agente de Rede

Sistemas operacionais. Microsoft Windows	Microsoft Windows Embedded POSReady 2009 com o Service Pack de 32 bits mais recente Microsoft Windows Embedded 7 Standard with Service Pack 1 32 bits/64 bits Microsoft Windows Embedded 8.1 Industry Pro 32 bits/64 bits Microsoft Windows 10 Enterprise 2015 LTSB 32 bits/64 bits Microsoft Windows 10 Enterprise 2016 LTSB 32 bits/64 bits Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 bits/64 bits Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 bits/64 bits Microsoft Windows 10 Enterprise 2019 LTSC 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1703 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1709 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1803 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1809 32 bits/64 bits Microsoft Windows 10 20H2 IoT Enterprise 32 bits/64 bits Microsoft Windows 10 21H2 IoT Enterprise 32 bits/64 bits Microsoft Windows 10 IoT Enterprise 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1909 32 bits/64 bits Microsoft Windows 10 IoT Enterprise LTSC 2021 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1607 32 bits/64 bits Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32 bits/64 bits Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32 bits/64 bits Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32 bits/64 bits Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32 bits/64 bits Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32 bits/64 bits Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32 bits/64 bits Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32 bits/64 bits Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32 bits/64 bits

Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32 bits/64 bits

Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32 bits/64 bits

Microsoft Windows 10 Home RS5 (outubro de 2018) 32 bits/64 bits

Microsoft Windows 10 Pro RS5 (outubro de 2018) 32 bits/64 bits

Microsoft Windows 10 Pro for Workstations RS5 (outubro de 2018) 32 bits/64 bits

Microsoft Windows 10 Enterprise RS5 (outubro de 2018) 32 bits/64 bits

Microsoft Windows 10 Education RS5 (outubro de 2018) 32 bits/64 bits

Microsoft Windows 10 Home 19H1 32 bits/64 bits

Microsoft Windows 10 Pro 19H1 32 bits/64 bits

Microsoft Windows 10 Pro for Workstations 19H1 32 bits/64 bits

Microsoft Windows 10 Enterprise 19H1 32 bits/64 bits

Microsoft Windows 10 Education 19H1 32 bits/64 bits

Microsoft Windows 10 Home 19H2 32 bits/64 bits

Microsoft Windows 10 Pro 19H2 32 bits/64 bits

Microsoft Windows 10 Pro for Workstations 19H2 32 bits/64 bits

Microsoft Windows 10 Enterprise 19H2 32 bits/64 bits

Microsoft Windows 10 Education 19H2 32 bits/64 bits

Microsoft Windows 10 Home 20H1 (Atualização de maio de 2020) 32 bits/64 bits

Microsoft Windows 10 Pro 20H1 (Atualização de abril de 2020) 32 bits/64 bits

Microsoft Windows 10 Enterprise 20H1 (Atualização de maio de 2020) 32 bits/64 bits

Microsoft Windows 10 Education 20H1 (Atualização de maio de 2020) 32 bits/64 bits

Microsoft Windows 10 Home 20H2 (Atualização de outubro de 2020) 32 bits/64 bits

Microsoft Windows 10 Pro 20H2 (Atualização de outubro de 2020) 32 bits/64 bits

Microsoft Windows 10 Enterprise 20H2 (Atualização de outubro de 2020) 32 bits/64 bits

Microsoft Windows 10 Education 20H2 (Atualização de outubro de 2020) 32 bits/64 bits

Microsoft Windows 10 Home 21H1 (Atualização de maio de 2021) 32 bits/64 bits

Microsoft Windows 10 Pro 21H1 (Atualização de abril de 2021) 32 bits/64 bits

Microsoft Windows 10 Enterprise 21H1 (Atualização de maio de 2021) 32 bits/64 bits

Microsoft Windows 10 Education 21H1 (Atualização de maio de 2021) 32 bits/64 bits

Microsoft Windows 10 Home 21H2 (Atualização de outubro de 2021) 32 bits/64 bits

Microsoft Windows 10 Pro 21H2 (Atualização de outubro de 2021) 32 bits/64 bits

Microsoft Windows 10 Enterprise 21H2 (Atualização de outubro de 2021) 32 bits/64 bits

Microsoft Windows 10 Education 21H2 (Atualização de outubro de 2021) 32 bits/64 bits

Microsoft Windows 10 Home 22H2 (atualização de outubro de 2023) 32/64 bits

Microsoft Windows 10 Pro 22H2 (atualização de outubro de 2023) 32/64 bits

Microsoft Windows 10 Enterprise 22H2 (atualização de outubro de 2023) 32/64 bits

Microsoft Windows 10 Education 22H2 (atualização de outubro de 2023) 32/64 bits

Microsoft Windows 11 Home 64 bits

Microsoft Windows 11 Pro 64 bits

Microsoft Windows 11 Enterprise 64 bits

Microsoft Windows 11 Education 64 bits

Microsoft Windows 11 22H2

Microsoft Windows 8.1 Pro 32 bits/64 bits

Microsoft Windows 8.1 Enterprise 32 bits/64 bits

Microsoft Windows 8 Pro 32 bits/64 bits

Microsoft Windows 8 Enterprise 32 bits/64 bits

Microsoft Windows 7 Professional com Service Pack 1 e versões posteriores de 32 bits/64 bits

Microsoft Windows 7 Enterprise/Ultimate com Service Pack 1 e versões posteriores de 32 bits/64 bits

Microsoft Windows 7 Home Basic/Premium com Service Pack 1 e versões posteriores de 32 bits/64 bits

Microsoft Windows XP Professional Service Pack 3 e versões posteriores de 32 bits

Microsoft Windows XP Professional for Embedded Systems Service Pack 3, 32 bits

Windows MultiPoint Server 2011 Standard/Premium 64 bits

Windows Server 2008 Foundation Service Pack 2 de 32 bits/64 bits

Windows Server 2008 Service Pack 2 (todas as edições) de 32 bits/64 bits

Windows Server 2008 R2 Datacenter Service Pack 1 e versões posteriores de 64 bits

Windows Server 2008 R2 Enterprise Service Pack 1 e versões posteriores de 64 bits

Windows Server 2008 R2 Foundation Service Pack 1 e versões posteriores de 64 bits

Windows Server 2008 R2 Core Mode Service Pack 1 e versões posteriores de 64 bits

Windows Server 2008 R2 Standard Service Pack 1 e versões posteriores de 64 bits

Windows Server 2008 R2 Service Pack 1 (todas as edições) 64 bits

Windows Server 2012 Server Core 64 bits

Windows Server 2012 Datacenter 64 bits

	Windows Server 2012 Essentials 64 bits Windows Server 2012 Foundation 64 bits Windows Server 2012 Standard 64 bits Windows Server 2012 R2 Server Core 64-bit Windows Server 2012 R2 Datacenter 64-bit Windows Server 2012 R2 Essentials 64 bits Windows Server 2012 R2 Foundation 64-bit Windows Server 2012 R2 Standard 64-bit Windows Server 2016 Datacenter (LTSB) 64 bits Windows Server 2016 Standard (LTSB) 64 bits Microsoft Windows Server 2016 Server Core (opção de Instalação) (LTSB) 64 bits Windows Server 2019 Standard 64 bits Windows Server 2019 Datacenter 64 bits Windows Server 2019 Core 64 bits Windows Server 2022 Standard 64 bits Windows Server 2022 Datacenter 64 bits Windows Server 2022 Core 64 bits
Sistemas operacionais. Linux	Debian GNU/Linux 12 (Bookworm) Debian GNU/Linux 11.x (Bullseye) 32 bits/64 bits Debian GNU/Linux 10.x (Buster) 32 bits/64 bits Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bits Ubuntu Server 20.04 LTS (Focal Fossa) 32 bits/64 bits Ubuntu Server 18.04 LTS (Bionic Beaver) 32 bits/64 bits CentOS Stream 9 64 bits CentOS 7.x 64 bits Red Hat Enterprise Linux Server 9.x 64 bits Red Hat Enterprise Linux Server 8.x 64 bits Red Hat Enterprise Linux Server 7.x 64 bits Red Hat Enterprise Linux Server 6.x 32 bits/64 bits SUSE Linux Enterprise Server 12 (todos Service Packs) 64 bits SUSE Linux Enterprise Server 15 (todos os Service Packs) 64 bits openSUSE 15 64 bits Oracle Linux 7 64 bits Oracle Linux 8 64 bits Oracle Linux 9 64 bits Linux Mint 20.x 64 bits
Sistemas operacionais macOS	macOS Big Sur (11.x) macOS Monterey (12.x) macOS Ventura (13.x)

Para o Agente de Rede, a arquitetura Apple Silicon (M1) também é compatível, assim como Intel.

As seguintes plataformas para virtualização são suportadas:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64 bits
- Microsoft Hyper-V Server 2012 R2 64 bits
- Microsoft Hyper-V Server 2016 64 bits
- Microsoft Hyper-V Server 2019 64 bits
- Microsoft Hyper-V Server 2022 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- Máquina virtual baseada em kernel (todos os sistemas operacionais Linux compatíveis com o Agente de Rede)

No Microsoft Windows XP, o Agente de Rede poderá não executar algumas operações corretamente.

Sistemas operacionais e plataformas incompatíveis

Agente de Rede

Os seguintes sistemas operacionais não são compatíveis:

- Microsoft Windows Embedded POSReady 7 32 bits/64 bits
- Microsoft Windows Embedded 8 Industry Pro 32 bits/64 bits
- Microsoft Windows Embedded 8 Industry Enterprise 32 bits/64 bits
- Microsoft Windows Embedded 8 Standard 32 bits/64 bits
- Microsoft Windows Embedded 8.1 Industry Enterprise 32 bits/64 bits

- Microsoft Windows Embedded 8.1 Industry Update 32 bits/64 bits
- Microsoft Windows 10 Home (Limite de 1, 1507) 32 bits/64 bits
- Microsoft Windows 10 Pro (Limite de 1, 1507) 32 bits/64 bits
- Microsoft Windows 10 Enterprise (Limite de 1, 1507) 32 bits/64 bits
- Microsoft Windows 10 Education (Limite de 1, 1507) 32 bits/64 bits
- Microsoft Windows 10 Mobile (Limite de 1, 1507) 32 bits
- Microsoft Windows 10 Mobile Enterprise (Limite de 1, 1507) 32 bits
- Microsoft Windows 10 Home Limite de 2 (November 2015 Update, 1511) 32 bits/64 bits
- Microsoft Windows 10 Pro Limite de 2 (November 2015 Update, 1511) 32 bits/64 bits
- Microsoft Windows 10 Enterprise Limite de 2 (November 2015 Update, 1511) 32 bits/64 bits
- Microsoft Windows 10 Education Limite de 2 (November 2015 Update, 1511) 32 bits/64 bits
- Microsoft Windows 10 Mobile Limite de 2 (November 2015 Update, 1511) 32 bits
- Microsoft Windows 10 Mobile Enterprise Limite de 2 (Novembro 2015 Update, 1511) 32 bits
- Microsoft Windows 10 Home RS1 (Anniversary Update, 1607) 32 bits/64 bits
- Microsoft Windows 10 Pro RS1 (Anniversary Update, 1607) 32 bits/64 bits
- Microsoft Windows 10 Enterprise RS1 (Anniversary Update, 1607) 32 bits/64 bits
- Microsoft Windows 10 Education RS1 (Anniversary Update, 1607) 32 bits/64 bits
- Microsoft Windows 10 Mobile RS1 (Anniversary Update, 1607) 32 bits
- Microsoft Windows 10 Mobile Enterprise RS1 (Anniversary Update, 1607) 32 bits
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32 bits/64 bits
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32 bits/64 bits
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32 bits/64 bits
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32 bits/64 bits
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32 bits
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32 bits
- Microsoft Windows 10 Mobile RS3 32 bits
- Microsoft Windows 10 Mobile Enterprise RS3 32 bits
- Microsoft Windows 10 Mobile RS4 32 bits

- Microsoft Windows 10 Mobile Enterprise RS4 32 bits
- Microsoft Windows 10 Mobile RS5 32 bits
- Microsoft Windows 10 Mobile Enterprise RS5 32 bits
- Microsoft Windows 8 (Core) 32 bits/64 bits
- Microsoft Windows 7 Professional 32 bits/64 bits
- Microsoft Windows 7 Enterprise/Ultimate 32 bits/64 bits
- Microsoft Windows 7 Home Basic/Premium 32 bits/64 bits
- Microsoft Windows Vista Business com Service Pack 1, 32 bits/64 bits
- Microsoft Windows Vista Enterprise com Service Pack 1 32 bits/64 bits
- Microsoft Windows Vista Ultimate com Service Pack 1, 32 bits/64 bits
- Microsoft Windows Vista Business com Service Pack 2 e versões posteriores 32 bits/64 bits
- Microsoft Windows Vista Enterprise com Service Pack 2 e versões posteriores 32 bits/64 bits
- Microsoft Windows Vista Ultimate com Service Pack 2 e versões posteriores 32 bits/64 bits
- Microsoft Windows XP Professional com Service Pack 2, 32 bits/64 bits
- Microsoft Windows XP Home com Service Pack 3 e posterior 32 bits
- Windows Essential Business Server 2008 Standard 64 bits
- Windows Essential Business Server 2008 Premium 64 bits
- Windows Small Business Server 2003 Standard com Service Pack 1 32 bits
- Windows Small Business Server 2003 Premium com Service Pack 1 32 bits
- Windows Small Business Server 2008 Standard 64 bits
- Windows Small Business Server 2008 Premium 64 bits
- Windows Small Business Server 2011 Premium Add-on 64 bits
- Windows Small Business Server 2011 Standard 64 bits
- Windows Small Business Server 2011 Essentials 64 bits
- Windows Home Server 2011 64 bits
- Windows MultiPoint Server 2010 Standard 64 bits
- Windows MultiPoint Server 2010 Premium 64 bits
- Windows MultiPoint Server 2012 Standard/Premium 64 bits

- Microsoft Windows 2000 Server 32 bits
- Windows Server 2003 Enterprise com Service Pack 2 de 32 bits/64 bits
- Windows Server 2003 Standard com Service Pack 2 de 32 bits/64 bits
- Windows Server 2003 R2 Enterprise com Service Pack 2 de 32 bits/64 bits
- Windows Server 2003 R2 Standard com Service Pack 2 de 32 bits/64 bits
- Windows Server 2008 Datacenter Service Pack 1 de 32 bits/64 bits
- Windows Server 2008 Enterprise Service Pack 1 de 32 bits/64 bits
- Windows Server 2008 Service Pack 1 Server Core de 32 bits/64 bits
- Windows Server 2008 Standard Service Pack 1 de 32 bits/64 bits
- Windows Server 2008 Standard de 32 bits/64 bits
- Microsoft Server 2008 Enterprise 32 bits/64 bits
- Windows Server 2008 Datacenter 32 bits/64 bits
- Windows Server 2008 R2 Server Core 64 bits
- Windows Server 2008 R2 Datacenter 64 bits
- Windows Server 2008 R2 Enterprise 64 bits
- Windows Server 2008 R2 Foundation 64 bits
- Windows Server 2008 R2 Standard 64 bits
- Windows Server 2016 Nano (Opção de Instalação) (CBB)
- Windows Storage Server 2008 32 bits/64 bits
- Windows Storage Server 2008 Service Pack 2 64 bits
- Windows Storage Server 2008 R2 64 bits
- Windows Storage Server 2012 64 bits
- Windows Storage Server 2012 R2 64 bits
- Windows Storage Server 2016 64 bits
- Windows Storage Server 2019 64 bits
- Debian GNU/Linux 7.x (até o 7.8) 32 bits/64 bits
- Debian GNU/Linux 8.x (Jessie) 32 bits/64 bits
- Debian GNU/Linux 9.x (Stretch) 32 bits/64 bits

- Ubuntu Server 14.04 LTS (Trusty Tahr) 32 bits/64 bits
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32 bits/64 bits
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32 bits/64 bits
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 bits/64 bits
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 bits
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 bits/64 bits
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 bits/64 bits
- CentOS 6.x (até 6.6) 64 bits
- CentOS 7.x ARM 64 bits
- CentOS 8.x 64 bits
- SUSE Linux Enterprise Desktop 12 (todos os SPs) 64 bits
- SUSE Linux Enterprise Desktop 15 (todos os Service Packs) 64 bits
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 bits
- ALT Server 10 64 bits
- ALT Server 9.2 64 bits
- ALT Workstation 10 32 bits/64 bits
- ALT Workstation 9.2 32 bits/64 bits
- ALT 8 SP Server (LKNV.11100-01) 64 bits
- ALT 8 SP Server (LKNV.11100-02) 64 bits
- ALT 8 SP Server (LKNV.11100-03) 64 bits
- ALT 8 SP Workstation (LKNV.11100-01) 32 bits/64 bits
- ALT 8 SP Workstation (LKNV.11100-02) 32 bits/64 bits
- ALT 8 SP Workstation (LKNV.11100-03) 32 bits/64 bits
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64 bits
- Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.7) de 64 bits
- Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.6) de 64 bits
- Astra Linux Common Edition (atualização operacional 2.12) de 64 bits

- Astra Linux Special Edition RUSB.10152-02 (atualização operacional 4.7) ARM de 64 bits
- Linux Mint 19.x 64 bits
- AlterOS 7.5 e versões posteriores de 64 bits
- Lotos (Linux core versão 4.19.50, DE: MATE) 64 bits
- Mageia 4 32 bits
- GosLinux IC6 64 bits
- RED OS 7.3 64 bits
- RED OS 7.3 Server 64 bits
- RED OS 7.3 Certified Edition 64 bits
- ROSA COBALT 7.9 64 bits
- ROSA CHROME 12 64 bits
- ROSA Enterprise Linux Server 7.3 64 bits
- ROSA Enterprise Linux Desktop 7.3 64 bits
- ROSA COBALT Workstation 7.3 64 bits
- ROSA COBALT Server 7.3 64 bit
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- macOS Sierra (10.12)
- macOS High Sierra (10.13)
- macOS Mojave (10.14)
- macOS Catalina (10.15)

As seguintes plataformas para virtualização são incompatíveis:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5

- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64 bits
- Microsoft Hyper-V Server 2008 R2 64 bits
- Microsoft Hyper-V Server 2008 R2 com Service Pack 1 e versões posteriores 64 bits
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

Aplicativos e soluções da Kaspersky compatíveis

Licenças para diferentes produtos habilitam diferentes conjuntos de aplicativos e soluções Kaspersky.

É possível implementar e gerenciar os seguintes aplicativos e soluções da Kaspersky por meio do Kaspersky Security Center Cloud Console:

- Kaspersky Security for Windows Server 11.0.1
- Kaspersky Endpoint Security 12.4 for Windows (somente a criptografia leve (AES56) é compatível)
- Kaspersky Endpoint Security 12.0 for Linux
- Kaspersky Endpoint Security for Mac versão 12 Patch A
- Kaspersky Embedded Systems Security 3.3 for Windows
- Kaspersky Embedded Systems Security 3.3 for Linux
- Kaspersky Endpoint Agent 3.16
- Kaspersky Endpoint Security for Android
- Kaspersky Security for iOS

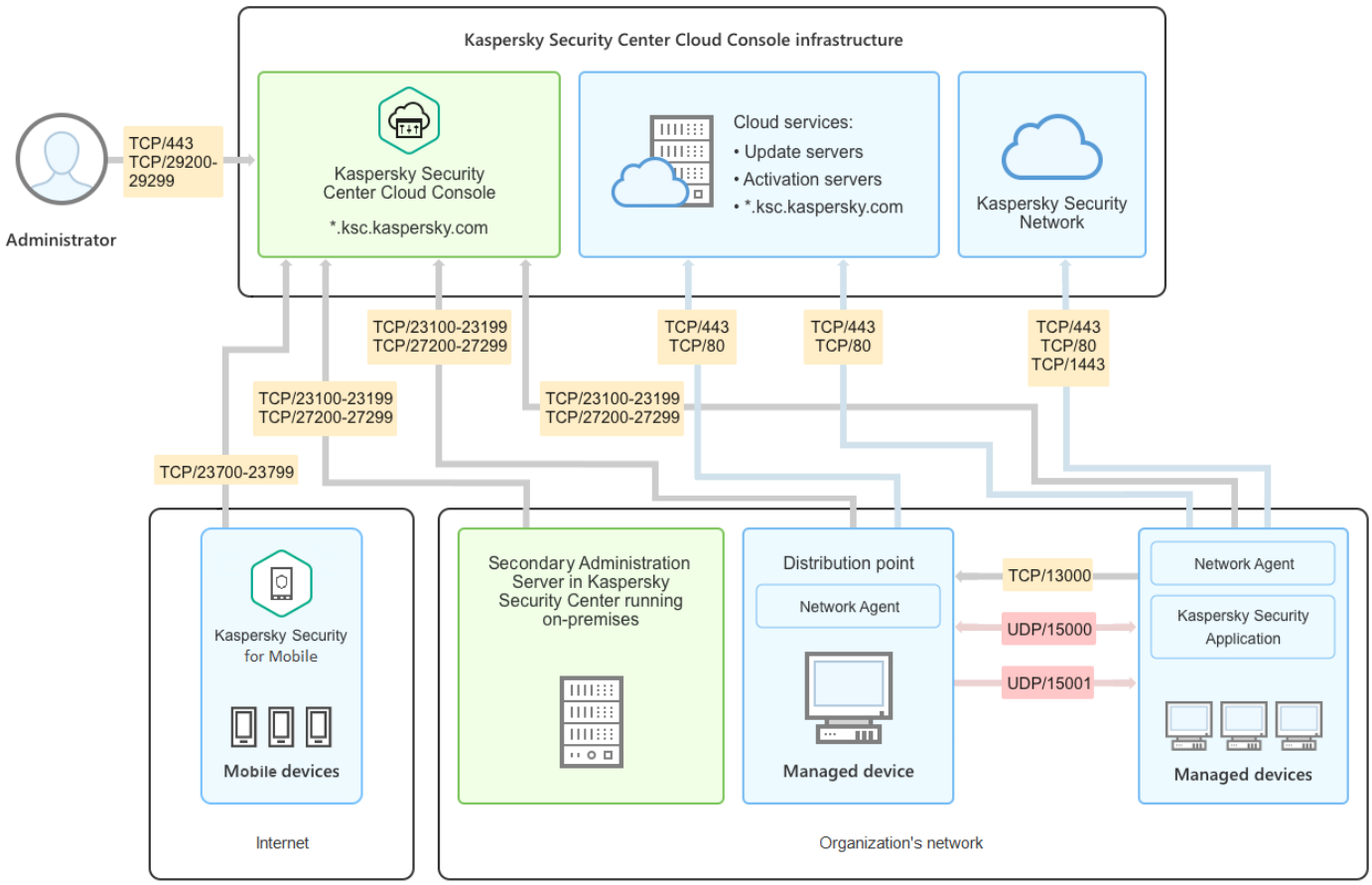
Você pode integrar as seguintes soluções para visualizar e processar incidentes de segurança:

- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Optimum 2.3
- Kaspersky Endpoint Detection and Response Expert

Se você instalar uma nova versão do aplicativo em um dispositivo gerenciado, mas usar uma política desatualizada em vez de atualizá-la, o aplicativo ainda fornecerá dados ao Kaspersky Security Center Cloud Console, mas não poderá processá-los conforme descrito na seção Dados processados de aplicativos gerenciados da documentação. Para que o Kaspersky Security Center Cloud Console processe esses dados, é necessário criar uma nova política para a nova versão do aplicativo.

Arquitetura

Esta seção fornece uma descrição dos componentes do Kaspersky Security Center Cloud Console e sua interação.



Arquitetura do Kaspersky Security Center Cloud Console

O Kaspersky Security Center Cloud Console gerenciado por meio do console baseado em nuvem inclui dois componentes principais: infraestrutura do Kaspersky Security Center Cloud Console e infraestrutura do cliente.

A infraestrutura do Kaspersky Security Center Cloud Console consiste no seguinte:

- **Console de Administração baseado em nuvem**. Fornece uma interface Web para criar e manter o sistema de proteção da rede de uma organização cliente gerenciada pelo Kaspersky Security Center Cloud Console.
- **Serviços na nuvem**. Inclui servidores de atualização e servidores de ativação.
- **Kaspersky Security Network (KSN)**. Servidores que contêm um banco de dados da Kaspersky com informações constantemente atualizadas sobre a reputação de arquivos, recursos da Web e software. O Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky quanto a ameaças, aprimora o desempenho de alguns componentes de proteção e reduz a probabilidade ocorrerem falsos positivos.

A infraestrutura do cliente pode consistir no seguinte:

- **Ponto de distribuição**. Um computador que tenha o Agente de Rede instalado e que é usado para a distribuição de atualizações, sondagem de rede, instalação remota de aplicativos, obtenção de informações sobre os computadores em um grupo de administração e/ou domínio de difusão. O administrador seleciona os dispositivos apropriados e atribui a eles pontos de distribuição manualmente.
- **Dispositivos gerenciados**. Computadores da rede do cliente protegidos pelo Kaspersky Security Center Cloud Console. O Agente de Rede e um aplicativo de segurança Kaspersky devem estar instalados em cada dispositivo gerenciado.
- **Servidor de administração secundário executado no local** (opcional). Você pode usar um Servidor de Administração local para criar uma hierarquia de Servidores de Administração.

Portas usadas pelo Kaspersky Security Center Cloud Console

Para usar o Kaspersky Security Center Cloud Console, que faz parte da infraestrutura da Kaspersky, é necessário abrir as seguintes portas nos dispositivos clientes para permitir a conexão com a Internet (consulte a tabela abaixo):

Portas que devem estar abertas nos dispositivos clientes para permitir a conexão com a Internet

Porta (ou intervalo de portas)	Protocolo	Finalidade da porta (ou intervalo de portas)
23100-23199	TCP/TLS	Conexões de recepção de Agentes de Rede e Servidores de Administração secundários no Servidor de Administração do Kaspersky Security Center Cloud Console no *.ksc.kaspersky.com. A infraestrutura Kaspersky pode usar qualquer porta dentro deste intervalo e qualquer endereço da web dentro desta máscara. A porta e o endereço da web podem mudar periodicamente.
23700-23799 (apenas se você gerencia dispositivos móveis)	TCP/TLS	Receber conexões de dispositivos móveis. Conexão com o servidor de administração do Kaspersky Security Center Cloud Console no *.ksc.kaspersky.com. A infraestrutura Kaspersky pode usar qualquer porta dentro deste intervalo e qualquer endereço da web dentro desta máscara. A porta e o endereço da web podem mudar periodicamente.
27200-27299	TCP/TLS	Conexões de recepção para a ativação do aplicativo de dispositivos gerenciados (exceto dispositivos móveis). Conexão com o servidor de administração do Kaspersky Security Center Cloud Console no *.ksc.kaspersky.com.

		A infraestrutura Kaspersky pode usar qualquer porta dentro deste intervalo e qualquer endereço da web dentro desta máscara. A porta e o endereço da web podem mudar periodicamente.
29200-29299	TCP/TLS	Tunelamento de conexões para dispositivos gerenciados usando o utilitário klsctunnel por meio do Servidor de Administração do Kaspersky Security Center Cloud Console em *.ksc.kaspersky.com. A infraestrutura Kaspersky pode usar qualquer porta dentro deste intervalo e qualquer endereço da web dentro desta máscara. A porta e o endereço da web podem mudar periodicamente.
443	HTTPS	Conexão com o serviço de descoberta do Kaspersky Security Center Cloud Console em *.ksc.kaspersky.com. A infraestrutura da Kaspersky pode usar qualquer endereço da Web nessa máscara.
1443	TCP	Conexão com a Kaspersky Security Network
80	TCP	A conexão é usada para verificar a validade dos certificados do Kaspersky Security Center em *.digicert.com. A infraestrutura da Kaspersky pode usar qualquer endereço da Web nessa máscara.

A tabela abaixo lista as portas que devem ser aberta nos dispositivos gerenciados onde o Agente de Rede está instalado.

Portas que devem estar abertas nos dispositivos clientes

Número da porta	Protocolo	Propósito da porta	Escopo
15000	UDP	Recebendo dados de gateways de conexão (se estiverem em uso)	Gerenciamento de dispositivos cliente
15000	Transmissão UDP	Obter dados sobre outros Agentes de Rede no mesmo domínio de transmissão	Entregar atualizações e pacotes de instalação
15001	UDP	Recebendo solicitações de multicast de um ponto de distribuição (se estiver em uso)	Recebendo atualizações e pacotes de instalação de um ponto de distribuição

Observe que o processo klnagent também pode solicitar portas livres do intervalo de portas dinâmicas de um sistema operacional de endpoint. Essas portas são alocadas automaticamente para o processo klnagent pelo sistema operacional. Assim, o processo klnagent poderá usar algumas portas que são usadas por outro software. Caso o processo klnagent afete as operações desse software, altere suas configurações da porta ou altere o intervalo padrão de porta dinâmica no sistema operacional para excluir a porta usada pelo software afetado.

Considere também que as recomendações sobre a compatibilidade do Kaspersky Security Center Cloud Console com softwares de terceiros são descritas apenas para referência e podem não ser aplicáveis a novas versões de softwares de terceiros. As recomendações descritas para configurar as portas são baseadas nas experiências do Suporte Técnico e em nossas práticas recomendadas.

A tabela abaixo lista as portas adicionais que devem ser abertas nos dispositivos clientes com o Agente de Rede instalado atuando como um ponto de distribuição.

Portas usadas pelo Agente de Rede funcionando como ponto de distribuição

Número da porta	Protocolo	Propósito da porta	Escopo
13000	TCP/TLS	Receber conexões dos Agentes de Rede	Gerenciar dispositivos cliente e entregar atualizações e

			pacotes de instalação
13111 (apenas se o serviço de Proxy da KSN for executado no dispositivo)	TCP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN
13295 (apenas se você usar o ponto de distribuição como um servidor push)	TCP/TLS	Enviando notificações push para dispositivos gerenciados	Ponto de distribuição usado como servidor push
15111 (apenas se o serviço de Proxy da KSN for executado no dispositivo)	UDP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN
17111 (apenas se o serviço de Proxy da KSN for executado no dispositivo)	HTTPS	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN

Caso tenha um ou mais Servidores de Administração em sua rede e os utilize como Servidores de Administração secundários quando o Servidor de Administração principal estiver localizado na infraestrutura da Kaspersky, consulte a lista de portas usadas pelo Kaspersky Security Center em execução no local. Use essas portas para interação entre o Servidor de Administração secundário (ou Servidores de Administração secundários) e os dispositivos clientes.

Interface do Kaspersky Security Center Cloud Console

O Kaspersky Security Center Cloud Console é gerenciado pela interface da Web.

A janela do aplicativo contém os seguintes itens:

- Menu principal na parte esquerda da janela
- Área de trabalho na parte direita da janela

Menu principal

O menu principal contém as seguintes seções:

- **Introdução e tutoriais**. Contém vídeos sobre como configurar e usar o Kaspersky Security Center Cloud Console e aplicativos de segurança.

  No navegador Mozilla Firefox, ao reproduzir um vídeo na seção **Introdução e tutoriais** na janela pop-up, abra o vídeo no modo quadro a quadro e feche o vídeo na janela pop-up, o vídeo no modo quadro a quadro também é fechado.

- **Servidor de Administração**. Exibe o nome do Servidor de Administração ao qual você está atualmente conectado. Clique no ícone de configurações ( ) para abrir as propriedades do Servidor de Administração.
- **Monitoramento e relatórios**. Esses recursos fornecem uma visão geral da infraestrutura, dos status de proteção e das estatísticas.

- **Ativos (dispositivos)**. Contém ferramentas para gerenciar dispositivos cliente, assim como tarefas e políticas do aplicativo Kaspersky.
- **Usuários e funções**. Permite gerenciar usuários e funções, configurar direitos de usuário atribuindo funções aos usuários e associar perfis de política com as funções.
- **Operações**. Contém uma variedade de operações, incluindo licenciamento de aplicativos, gerenciamento de patches e gerenciamento de aplicativos de terceiros. Isso também fornece acesso aos repositórios de aplicativos.
- **Descoberta e implementação**. Permite fazer a sondagem da rede para descobrir dispositivos cliente e distribuir os dispositivos para grupos de administração manual ou automaticamente. Ele também contém o Assistente de início rápido e o Assistente de implementação da proteção.
- **Marketplace**. Contém informações sobre toda a gama de soluções empresariais da Kaspersky e permite a seleção das soluções necessárias e, em seguida, prossegue para a compra dessas soluções no site da Kaspersky.
- **Configurações**. Contém configurações para integrar o Kaspersky Security Center Cloud Console com outros aplicativos da Kaspersky. Ele também contém suas configurações pessoais relacionadas à aparência da interface, como idioma ou tema da interface.
- **O menu da sua conta**. Contém um link para a ajuda on-line e informações sobre o Suporte Técnico da Kaspersky. Ele também permite sair do Kaspersky Security Center Cloud Console.

Área de trabalho

A área de trabalho exibe as informações escolhidas para serem visualizadas nas seções da janela da interface da Web do aplicativo. Ela também contém elementos de controle que podem ser usados para configurar como as informações são exibidas.

Localização do Kaspersky Security Center Cloud Console

A interface e a documentação do Kaspersky Security Center Cloud Console estão disponíveis nos seguintes idiomas:

- Inglês
- Francês
- Alemão
- Italiano
- Japonês
- Português (Brasil)
- Russo
- Espanhol
- Espanhol (LATAM)

Comparação entre o Kaspersky Security Center e o Kaspersky Security Center Cloud Console

É possível usar o Kaspersky Security Center das seguintes maneiras:

- Como uma solução em nuvem

  O Kaspersky Security Center é instalado para você no ambiente em nuvem e a Kaspersky fornece acesso ao Servidor de Administração como um serviço. Você gerencia o sistema de segurança da rede através do Console de Administração baseado na nuvem chamado Kaspersky Security Center Cloud Console. Esse console tem uma interface semelhante à interface do Kaspersky Security Center Web Console.

- Como uma solução local (baseada em Windows ou Linux)

  Você instala o Kaspersky Security Center em um dispositivo local e gerencia o sistema de segurança de rede usando o Console de Administração baseado no Console de Gerenciamento Microsoft ou no Kaspersky Security Center Web Console.

  Além do aplicativo baseado no Windows, o Kaspersky Security Center Linux também está disponível. O Kaspersky Security Center Linux foi projetado para implementar e gerenciar a proteção de dispositivos Linux usando o Servidor de Administração baseado em Linux para atender aos requisitos de ambientes exclusivamente Linux. O Kaspersky Security Center e o Kaspersky Security Center Linux baseados em Windows possuem diferentes conjuntos de recursos.

A tabela abaixo permite comparar os principais recursos do Kaspersky Security Center e do Kaspersky Security Center Cloud Console.

Comparação dos recursos do Kaspersky Security Center executado no local com os recursos de uma solução na nuvem

Recurso ou propriedade	Kaspersky Security Center 14 em execução no local	Kaspersky Security Center Cloud Console
Localização do Servidor de Administração	No local	Nuvem
Localização do sistema de gerenciamento de banco de dados (DBMS)	No local	Nuvem
Console de administração baseado na Web	✓	✓
Manutenção do Servidor de Administração e do DBMS	Gerenciado pelo cliente	Gerenciado pela Kaspersky
Hierarquia de Servidores de Administração	✓	✓ (O servidor de administração do Kaspersky Security Center Cloud Console pode atuar apenas como um Servidor de administração principal na hierarquia e pode ser usado apenas para o monitoramento de políticas e tarefas)
Hierarquia do grupo de administração	✓	✓
Migração dos dispositivos gerenciados e objetos relacionados	✓	✓

do Kaspersky Security Center no local para o Kaspersky Security Center Cloud Console		
Sondagem da rede	✓	✓ (apenas por pontos de distribuição)
Número máximo de dispositivos gerenciados	100.000	25.000
Proteção de dispositivos gerenciados Windows, Linux e macOS	✓	✓
Proteção de dispositivos móveis	✓	✓ (somente o Kaspersky Endpoint Security for Android e o Kaspersky Security for iOS são compatíveis)
Proteção da infraestrutura de nuvem pública	✓	✓
Gerenciamento de segurança centrada no dispositivo	✓	✓
Políticas do aplicativo	✓	✓
Tarefas para aplicativos da Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
Servidor Proxy da KSN	✓	✓ (apenas em pontos de distribuição)
Kaspersky Private Security Network	✓	–
Implementação centralizada de chaves de licença para aplicativos da Kaspersky	✓	✓
Mudar os dispositivos gerenciados para outro Servidor de administração	✓	– (é necessário reinstalar os Agentes de rede nos dispositivos gerenciados para mudá-los para outro Servidor de administração)
Suporte para Servidores de administração virtuais	✓	✓
Instalar atualizações de softwares de terceiros e corrigir vulnerabilidades de softwares de terceiros	✓	✓ (para corrigir vulnerabilidades de software de terceiros, apenas as correções recomendadas podem ser instaladas)
Notificações sobre eventos ocorridos em dispositivos gerenciados	✓	✓
Criação e gerenciamento de contas de usuário	✓	✓
Número máximo de eventos no banco de dados	400.000 (pode ser aumentado até 45.000.000)	400.000 (depende do número de dispositivos gerenciados)

Integração com sistemas SIEM	✓	✓ (usando apenas o formato Syslog e o protocolo TLS sobre TCP)
Usar Servidor de Administração como servidor WSUS	✓	–
Monitoramento dos status de políticas e tarefas	✓	✓
Suporte a clusters e matrizes de servidores em grupos de administração	✓ (apenas no Console de Administração baseado em MMC)	–
Instalação remota de sistemas operacionais	✓	–
Suporte para SNMP	✓	–
Número máximo de Servidores virtuais	500	200

Conceitos básicos

Esta seção explica os conceitos básicos relacionados com o Kaspersky Security Center Cloud Console.

Agente de Rede

A interação entre o Servidor de Administração e os dispositivos é realizada pelo componente *Agente de Rede* do Kaspersky Security Center Cloud Console. O Agente de Rede deve ser instalado em todos os dispositivos cliente, nos quais o Kaspersky Security Center Cloud Console é usado para gerenciar os aplicativos da Kaspersky.

O Agente de Rede é instalado no dispositivo como um serviço com o seguinte conjunto de atributos:

- Com o nome "Agente de Rede do Kaspersky Security Center"
- Configurado para iniciar automaticamente ao inicializar o sistema operacional
- Usar o LocalSystem Account

Um dispositivo com o Agente de Rede instalado é denominado de *dispositivo gerenciado* ou *dispositivo*. Você pode instalar o Agente de Rede em um dispositivo Windows, Linux ou Mac.

O nome do processo que o Agente de Rede inicia é *klnagent.exe*.

O Agente de Rede sincroniza o dispositivo gerenciado com o Servidor de Administração. O Kaspersky Security Center Cloud Console sincroniza automaticamente várias vezes por hora o Servidor de Administração com os dispositivos gerenciados. O Servidor de Administração define o intervalo de sincronização (também conhecido como *heartbeat*) dependendo do número de dispositivos gerenciados.

Grupos de administração

Um *grupo de administração* (aqui também referido como um *grupo*) é um conjunto lógico de dispositivos gerenciados combinados na base de um tratado específico com o propósito de gerenciar os dispositivos agrupados como uma unidade única dentro do Kaspersky Security Center Cloud Console.

Todos os dispositivos gerenciados dentro de um grupo de administração são configurados para fazer o seguinte:

- Usar as mesmas configurações de aplicativo (que você pode definir nas políticas de grupo).
- Use um modo de operação comum para todos os aplicativos por meio da criação de tarefas de grupo com configurações especificadas. Exemplos de tarefas de grupo incluem criar e instalar um pacote de instalação comum, atualizar os bancos de dados e módulos de aplicativos, verificar dispositivo sob demanda e ativar a proteção em tempo real.

Um dispositivo gerenciado pode pertencer a um somente grupo de administração.

Você pode criar hierarquias que têm qualquer grau de aninhamento para Servidores de Administração e grupos. Um único nível de hierarquia pode incluir servidores de administração secundários e virtuais, grupos e dispositivos gerenciados. Você pode migrar dispositivos de um grupo ao outro sem movê-los fisicamente. Por exemplo, se o cargo de um funcionário na empresa for alterado de contador para desenvolvedor, você pode mover o computador desse funcionário do grupo de administração Contadores para o grupo de administração Desenvolvedores. Depois disso, o computador receberá automaticamente as configurações de aplicativo necessárias para desenvolvedores.

Hierarquia de Servidores de Administração

Os Servidores de Administração podem ser dispostos na hierarquia "principal/secundário". Cada Servidor de Administração pode possuir vários Servidores de Administração secundários em diferentes níveis de alojamento da hierarquia. O nível de alojamento para Servidores de Administração secundários é ilimitado. Os grupos de administração do Servidor de Administração principal incluirão então os dispositivos cliente de todos os Servidores de Administração secundários.

O Servidor de Administração do Kaspersky Security Center Cloud Console pode atuar apenas como um Servidor de Administração principal e pode ter como servidores secundários apenas os Servidores de Administração em execução no local.

Ao migrar do Servidor de Administração executado no local para o Servidor de Administração do Kaspersky Security Center Cloud Console, é possível organizar os Servidores de Administração em uma hierarquia. Em seguida, para reduzir a migração, é possível mudar apenas parte dos dispositivos gerenciados para o gerenciamento do Servidor de Administração do Kaspersky Security Center Cloud Console. O restante dos dispositivos gerenciados permanece sob o gerenciamento do Servidor de Administração local. Isso permite testar os recursos de gerenciamento do Kaspersky Security Center Cloud Console em um número limitado de dispositivos gerenciados. Ao mesmo tempo, é possível configurar políticas, tarefas, relatórios e outros objetos para testar o gerenciamento e o monitoramento de toda a rede. Isso permite voltar aos objetos configurados no Servidor de Administração local, se necessário.

Cada dispositivo incluído na hierarquia dos grupos de administração pode ser conectado apenas a um Servidor de Administração. Você deve monitorar de forma independente a conexão de dispositivos aos Servidores de Administração. Use o recurso para a pesquisa de dispositivos em grupos de administração de diferentes Servidores de Administração com base em atributos de rede.

Servidor de Administração virtual

O Servidor de Administração virtual (também referido como *Servidor virtual*) é um componente do Kaspersky Security Center Cloud Console projetado para gerenciar a proteção antivírus da rede de uma organização cliente. Cada Servidor de Administração virtual pode ter sua própria estrutura de grupos de administração e seus próprios meios de gerenciamento e monitoramento, como políticas, tarefas, relatórios e eventos. O escopo funcional dos Servidores de Administração virtuais pode ser usado por organizações com fluxos de trabalho complicados.

O Servidor de Administração virtual possui as seguintes restrições:

- Os servidores de administração virtual são compatíveis apenas com o modo comercial do Kaspersky Security Center Cloud Console.

- O Servidor de Administração virtual não é compatível com a criação de Servidores de Administração secundários (incluindo servidores virtuais).
- Você não pode migrar os Servidores de Administração virtuais do Kaspersky Security Center para o Kaspersky Security Center Cloud Console.
- Os servidores de administração virtual não podem ser gerenciados por administradores dedicados. Por padrão, o administrador que gerencia o Servidor de Administração principal também gerencia todos os Servidores de Administração virtuais.
- Os usuários criados em um servidor virtual não podem receber uma função no Servidor de Administração.
- Na janela de propriedades do Servidor de Administração virtual, o número de seções é limitado.

Ponto de distribuição

Ponto de distribuição é um dispositivo com o Agente de Rede instalado, que é usado para a distribuição da atualização, a instalação remota de aplicativos e a recuperação de informações sobre os dispositivos na rede. Um ponto de distribuição pode executar as seguintes funções:

- Distribuir as atualizações e os pacotes de instalação recebidos nos dispositivos cliente no grupo (incluindo distribuição por meio de multicasting usando UDP). As atualizações podem ser recebidas dos servidores de atualização da Kaspersky por meio de uma tarefa de atualização criada para o ponto de distribuição.

  Os dispositivos de ponto de distribuição executando macOS não podem baixar atualizações dos servidores de atualização da Kaspersky.

  > Se um ou mais dispositivos executando macOS estiverem dentro do escopo da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a tarefa será concluída com o status *Falha*, mesmo se for concluída com êxito em todos os dispositivos Windows.

- Distribuir políticas e tarefas de grupo através de multicasting usando UDP.
- Atua como um gateway para conexão ao Servidor de Administração para dispositivos em um grupo de administração.

  Se não for possível estabelecer uma conexão direta entre os dispositivos gerenciados no grupo e o Servidor de Administração, o ponto de distribuição pode ser usado como um gateway de conexão para o Servidor de Administração para esse grupo. Nesse caso, os dispositivos gerenciados serão conectados ao gateway de conexão, o qual, por sua vez, será conectado ao Servidor de Administração.

  A presença de um ponto de distribuição que opera como um gateway de conexão não bloqueia a opção de conexão direta entre os dispositivos gerenciados e o Servidor de Administração. Se o gateway de conexão não estiver disponível, mas a conexão direta com o Servidor de Administração for tecnicamente possível, os dispositivos gerenciados serão conectados ao Servidor de Administração diretamente.

- Faça a sondagem da rede para detectar novos dispositivos e para atualizar as informações sobre os existentes.
- Execute uma instalação remota do software de terceiros e de aplicativos Kaspersky usando as ferramentas do Microsoft Windows, incluindo a instalação nos dispositivos cliente sem o Agente de Rede.

  Este recurso permite a transferência remota de pacotes de instalação do Agente de Rede para dispositivos cliente localizados em redes às quais o Servidor de Administração não tem acesso direto.

- Atua como um servidor proxy que participa do Kaspersky Security Network.

Esse recurso não tem suporte de dispositivos de ponto de distribuição executando Linux ou macOS.

Você pode ativar o servidor proxy da KSN no lado do ponto de distribuição para fazer o dispositivo funcionar como um servidor proxy da KSN. Neste caso, o serviço de Proxy da KSN (ksnproxy) é executado no dispositivo.

Os Arquivos são transmitidos do Servidor de Administração a um ponto de distribuição através de HTTP ou, se a Conexão SSL estiver ativada, através de HTTPS. Usar HTTP ou HTTPS resulta em um desempenho mais alto, comparando com o SOAP, através da redução de tráfego.

Os dispositivos com o Agente de Rede instalado devem receber pontos de distribuição manualmente, de acordo com os grupos de administração. A lista completa de pontos de distribuição para grupos de administração especificados é exibida no relatório na lista de pontos de distribuição.

O escopo de um ponto de distribuição é o grupo de administração ao qual ele foi atribuído pelo administrador, assim como seus subgrupos de todos os níveis de incorporação. No entanto, o dispositivo que atua como o ponto de distribuição não pode estar incluído no grupo de administração ao qual foi atribuído. Se múltiplos pontos de distribuição tiverem sido atribuídos na hierarquia de grupos de administração, o Agente de Rede do dispositivo gerenciado se conecta ao ponto de distribuição mais próximo na hierarquia.

Uma localização da rede também pode ser o escopo dos pontos de distribuição. A localização da rede é então usada para a criação manual de um conjunto de dispositivos ao qual o ponto de distribuição distribuirá as atualizações. A localização da rede somente pode ser determinada para dispositivos que executam um sistema operacional Windows.

O Kaspersky Security Center Cloud Console atribui a cada Agente de Rede um endereço IP multicast único que se diferencia de cada outro endereço. Isto permite evitar a sobrecarga de rede que poderia ser causada por sobreposições de IP.

Quando dois ou mais pontos de distribuição forem atribuídos à uma única área de rede ou para um único grupo de administração, um deles se torna o ponto de distribuição ativo, e o restante deles se tornam pontos de distribuição em standby. O ponto de distribuição ativo baixa as atualizações e os pacotes de instalação diretamente do Servidor de Administração, enquanto os pontos de distribuição em standby recuperam as atualizações somente do ponto de distribuição ativo. Neste caso, após os arquivos terem sido baixados do Servidor de Administração eles são distribuídos entre os pontos de distribuição. Se o ponto de distribuição ativo se tornar indisponível por qualquer motivo, um dos pontos de distribuição independentes se torna ativo. O Servidor de Administração atribui automaticamente um ponto de distribuição para agir como standby.

O status do ponto de distribuição (*Ativo/Standby*) é exibido com uma caixa de seleção no relatório klnagchk.

Um ponto de distribuição requer ao menos 4 GB de espaço livre no disco. Caso o espaço em disco disponível do ponto de distribuição seja menor do que 2 GB, o Kaspersky Security Center Cloud Console cria um incidente de segurança com o nível de importância de *Advertência*. O problema de segurança será publicado nas propriedades do dispositivo, na seção **Problemas de segurança**.

Executando tarefas de instalação remotas em um dispositivo atribuído como um ponto de distribuição necessita de espaço em disco disponível livre adicional. O volume do espaço em disco disponível livre deve exceder o tamanho total de todos os pacotes de instalação a ser instalados.

Executando qualquer tarefa de atualização (correção) e de correção de vulnerabilidades em um dispositivo atribuído como um ponto de distribuição necessita de espaço em disco disponível livre adicional. O volume do espaço em disco disponível livre deve ser pelo menos duas vezes o tamanho total de todos os patches a serem instalados.

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Plug-in da Web de gerenciamento

Um componente especial, o *plugin de gerenciamento da Web*, é usado para a administração remota de softwares da Kaspersky por meio do Kaspersky Security Center Web Console. No presente documento, o plug-in da Web de gerenciamento será referido como *plug-in de gerenciamento*. Um plugin de gerenciamento é uma interface entre o Kaspersky Security Center Cloud Console e um aplicativo da Kaspersky específico. Com um plug-in de gerenciamento, você pode configurar tarefas e políticas para o aplicativo.

O plug-in de gerenciamento fornece o seguinte:

- Interface para criar e editar tarefas e configurações de aplicativo
- Interface para criar e editar políticas e perfis da política para a configuração remota e centralizada de aplicativos e dispositivos da Kaspersky
- Transmissão de eventos gerados pelo aplicativo
- Funções do Kaspersky Security Center Cloud Console para exibir os dados operacionais e os eventos do aplicativo, além das estatísticas transmitidas dos dispositivos cliente

Políticas

Uma *política* é um conjunto de configurações do aplicativo Kaspersky, aplicadas a um grupo de administração e seus subgrupos. Você pode instalar vários aplicativos Kaspersky nos dispositivos de um grupo de administração. O Kaspersky Security Center Cloud Console fornece uma única política para cada aplicativo Kaspersky em um grupo de administração. Uma política tem um dos seguintes status (consulte a tabela abaixo):

O status da política

Status	Descrição
Ativo	A política atual aplicada ao dispositivo. Apenas uma política pode estar ativa por aplicativo Kaspersky em cada grupo de administração. Os dispositivos aplicam os valores de configuração de uma política ativa para um aplicativo Kaspersky.
Inativo	Uma política que não é aplicada atualmente a um dispositivo.
Ausência	Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

As políticas funcionam de acordo com as seguintes regras:

- Várias políticas com valores diferentes podem ser configuradas para um único aplicativo.
- Apenas uma política pode estar ativa para o aplicativo atual.
- É possível ativar uma política desativada quando um evento específico ocorre. Por exemplo, você pode forçar configurações de proteção antivírus mais rigorosas durante surtos de vírus.
- Uma política pode ter políticas secundárias.

Geralmente, você pode usar políticas como preparação para situações de emergência, como um ataque de vírus. Se houver um ataque por meio de unidades flash, você pode ativar uma política que bloqueie o acesso a unidades flash. Nesse caso, a política ativa atual torna-se automaticamente inativa.

Para evitar ter que efetuar manutenção de várias políticas, por exemplo, quando ocasiões diferentes pressupõem a alteração de várias configurações apenas, você pode usar perfis de política.

Um *perfil de política* é um subconjunto nomeado de valores de configuração que substitui os valores de configuração de uma política. Um perfil de política afeta a formação de configurações efetivas em um dispositivo gerenciado. *Configurações em vigor* são um conjunto de configurações de política, configurações de perfil de política e configurações de aplicativo locais aplicadas atualmente ao dispositivo.

Os perfis de política funcionam de acordo com as seguintes regras:

- Um perfil de política entra em vigor quando ocorre uma condição de ativação específica.
- Os perfis contêm valores de configurações que diferem das configurações de política.
- A ativação de um perfil de política altera as configurações em vigor do dispositivo gerenciado.
- Uma política pode incluir no máximo 100 perfis de política.

Perfis da política

Às vezes pode ser necessário criar diversas instâncias de uma única política para diferentes grupos de administração; também convém sincronizar os as configurações dessas políticas centralmente. Essas instâncias podem diferir por apenas uma ou duas configurações. Por exemplo, todos os contadores em uma empresa trabalham segundo a mesma política, mas os contadores sênior estão autorizados a usar unidades flash e os contadores júnior, não. Neste caso, aplicar políticas aos dispositivos somente através da hierarquia de grupos de administração pode ser inconveniente.

Para ajudar a evitar a criação de várias instâncias de uma única política, o Kaspersky Security Center Cloud Console permite criar *perfis de política*. Os perfis de política são destinados se você quiser que os dispositivos dentro de um grupo de administração único executem sob configurações de política diferentes.

Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos alvo em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo gerenciado. A ativação de um perfil modifica as configurações da política "básica" que estavam inicialmente ativas no dispositivo. As configurações modificadas assumem valores que foram especificados no perfil.

Como as configurações do aplicativo local se relacionam com as políticas

Você pode usar as políticas para definir valores idênticos das configurações do aplicativo para todos os dispositivos no grupo.

Os valores das configurações especificados por uma política podem ser redefinidos para dispositivos individuais em um grupo usando as configurações do aplicativo locais. Você somente pode definir os valores das configurações, cuja alteração seja permitida pela política, ou seja, configurações desbloqueadas.

O valor de uma configuração que um aplicativo usa em um dispositivo cliente é definido pela posição do cadeado ( ) para aquela configuração na política:

- Se a modificação da configuração estiver bloqueada, o mesmo valor (definido na política) é utilizado e todos os dispositivos cliente.

- Se a modificação da configuração estiver desbloqueada, o aplicativo usa um valor de configuração local em cada dispositivo cliente em vez do valor especificado na política. O valor do parâmetro pode então ser alterado nas configurações de aplicativo locais.

Deste modo, quando a tarefa está sendo executada em um dispositivo cliente, o aplicativo usa as configurações definidas de duas formas diferentes:

- Por configurações de tarefa e configurações locais de aplicativo, se a configuração não estiver bloqueada contra alteração na política.

- Por política de grupo, se a configuração estiver bloqueada contra alteração.

As configurações de aplicativo locais são alteradas depois da primeira imposição de política de acordo com as configurações de política.

Licenciamento do aplicativo

Esta seção fornece informações relacionadas ao licenciamento de aplicativos.

Licenciamento do Kaspersky Security Center Cloud Console: cenário

Seguindo este cenário, você pode começar a usar o Kaspersky Security Center Cloud Console e os aplicativos de segurança gerenciados sob uma licença.

O Kaspersky Security Center Cloud Console permite realizar a distribuição centralizada de chaves de licença para os aplicativos Kaspersky em dispositivos clientes, monitorar o uso e renovar licenças.

Se você já estiver usando o Kaspersky Security Center Cloud Console, visite o Kaspersky Marketplace e confira toda a gama de soluções comerciais da Kaspersky, selecione as que você precisa e prossiga para a compra no site da Kaspersky.

Conhecendo os recursos do Kaspersky Security Center Cloud Console no modo avaliação antes de comprar uma licença

Você pode experimentar o Kaspersky Security Center Cloud Console gratuitamente, antes de comprar. Para isso, crie um espaço de trabalho de avaliação com duração de 30 dias. Se quiser um espaço de trabalho comercial para usar por tempo ilimitado, adquira uma licença.

O modo de avaliação não lhe permite alternar posteriormente para o modo comercial. Qualquer espaço de trabalho de avaliação será excluído automaticamente com todo o seu conteúdo quando o prazo de 30 dias expirar.

Fases

O cenário continua em estágios:

1. **Obtendo um código de ativação para licenciar o Kaspersky Security Center Cloud Console no modo comercial. Adquirindo uma ou mais licenças**

   Licenças diferentes permitem o uso de aplicativos e serviços diferentes da Kaspersky, por isso você pode precisar de mais de uma licença.

   Descubra quais licenças você deseja comprar e a quantidade mínima de dispositivos para cada licença.

   Kaspersky Security Center Cloud Console é parte integrante de várias soluções Kaspersky. Escolha a solução que deseja usar e adquira uma licença correspondente. Contate a Kaspersky ou um dos parceiros Kaspersky para fazer uma solicitação especial, se quiser comprar uma licença para 10.000 ou mais dispositivos.

   Consulte a tabela para verificar quais recursos de Gerenciamento de patches e vulnerabilidades estão disponíveis.

   Se deseja usar o Kaspersky Security Center Cloud Console em um ambiente de nuvem como o Microsoft Azure, leia sobre as opções de licenciamento para ambientes em nuvem.

   Se você representa um provedor de serviços gerenciados (MSP), leia sobre o licenciamento do Kaspersky Security Center Cloud Console para MSPs.

2. **Ativação do Kaspersky Security Center Cloud Console ao criar o espaço de trabalho**

Você especifica sua chave de licença para ativar o Kaspersky Security Center Cloud Console ao criar um espaço de trabalho.

Se você tiver mais de uma chave de licença, especifique qualquer uma delas e, posteriormente, deve adicionar outras chaves de licença no Kaspersky Security Center Cloud Console para ativar os aplicativos Kaspersky gerenciados.

3. **Adicionando chaves de licença para aplicativos gerenciados ao Servidor de Administração**

   Antes da implementação das chaves de licença, você deve adicionar essas chaves de licença ao repositório do Servidor de Administração.

   A chave de licença especificada ao criar a área de trabalho é automaticamente adicionada ao repositório do Servidor de Administração.

   Se você tiver mais de uma chave de licença, adicione as chaves de licença, uma por uma ao repositório do servidor de administração do Kaspersky Security Center Cloud Console.

4. **Implementando chaves de licença para aplicativos gerenciados**

   Escolha um método de implementação de uma ou mais chaves de licença para todos os dispositivos que deseja proteger:

   - Implementação automática

     > Caso diferentes aplicativos gerenciados sejam usados e seja necessário implementar um código de ativação específico para eles, escolha outra maneira de implementar esse código de ativação.

     O Kaspersky Security Center permite implementar automaticamente as chaves de licença disponíveis nos aplicativos gerenciados. Por exemplo, três chaves de licença são armazenadas no repositório do Servidor de Administração. Se você habilitou a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados** para todas as três chaves de licença. Um aplicativo de segurança da Kaspersky – por exemplo, Kaspersky Endpoint Security for Windows – é instalado nos dispositivos da organização. Um novo aplicativo gerenciado é detectado para o qual uma chave de licença deve ser implementada. Por exemplo, duas das chaves de licença do repositório podem ser implementadas para o aplicativo gerenciado no dispositivo: a chave de licença denominada *Key_1*e a denominada *Key_2*. Uma destas chaves de licença é implementada para o aplicativo gerenciado. Neste caso, não pode ser previsto qual das duas chaves de licença será implementada porque a implementação automática de chaves de licença não é fornecida para nenhuma atividade do administrador.

     Quando uma chave de licença é implementada, a quantidade de instalações é recontada para aquela chave de licença. Você deve certificar-se de que o número de aplicativos nos quais a chave de licença foi implementada não excede o limite da licença. Se a quantidade de dispositivos exceder o limite de licença, todos os dispositivos que não foram cobertos pela licença terão o status *Crítico* atribuído.

     Instruções de como proceder:

     - Adição de uma chave de licença ao repositório do Servidor de Administração
     - Distribuição automática de uma chave de licença

   - Implementação através da tarefa de adicionar uma chave de licença para um aplicativo gerenciado

     Se você optar por usar a tarefa Adicionar chave de licença para um aplicativo gerenciado, poderá selecionar a chave de licença a ser implementada nos dispositivos e selecionar os dispositivos da maneira mais conveniente, por exemplo, selecionando um grupo de administração ou uma seleção de dispositivos.

     Instruções de como proceder:

     - Adição de uma chave de licença ao repositório do Servidor de Administração
     - Implementando uma chave de licença para dispositivos cliente

- Adicionar um código de ativação ou um arquivo de chave manualmente nos dispositivos

  Você pode ativar o aplicativo da Kaspersky instalado localmente usando as ferramentas fornecidas na interface do aplicativo. Consulte a documentação do aplicativo instalado.

5. **Verificando em quais dispositivos os aplicativos gerenciados Kaspersky estão ativados**

   Para garantir que as chaves de licença sejam implementadas corretamente, consulte a lista das chaves de licença usadas para um aplicativo.

6. **Configurando eventos relacionados à expiração da licença**

   Configure eventos para receber notificações quando as chaves de licença estiverem vencidas ou prestes a expirar:

   - Eventos críticos do Servidor de Administração
   - Eventos de falha funcional do Servidor de Administração
   - Eventos de aviso do Servidor de Administração
   - Eventos informativos do Servidor de Administração

Sobre o modo de avaliação do Kaspersky Security Center Cloud Console

O *modo de avaliação* é um modo especial do Kaspersky Security Center Cloud Console, destinado à familiarização do usuário com os recursos do Kaspersky Security Center Cloud Console. Neste modo, é possível executar as atividades em um espaço de trabalho cujo período de validade está limitado a 30 dias. O modo de avaliação é ativado automaticamente assim que um espaço de trabalho de avaliação é criado. O conjunto de recursos disponíveis no modo de avaliação é idêntico ao escopo sob a licença padrão do Kaspersky Endpoint Security for Business Advanced.

No Kaspersky Security Center Cloud Console, não é necessário licenciar o Servidor de Administração, pois não há suporte para os recursos que exigem uma licença especial. Caso deseje usar o Kaspersky Security Center Cloud Console no modo de avaliação, você receberá uma licença de avaliação automaticamente ao criar o primeiro espaço de trabalho.

O modo de avaliação não lhe permite alternar posteriormente para o modo comercial. Qualquer espaço de trabalho de avaliação será excluído automaticamente com todo o seu conteúdo quando o prazo de 30 dias expirar.

As seguintes restrições são impostas ao uso dos recursos do Kaspersky Security Center Cloud Console no modo de avaliação:

- Você não pode criar uma hierarquia de Servidores de Administração. Nenhum servidor de administração virtual pode ser criado.
- A seção **Licenciamento** está disponível como somente leitura. Todas as operações são proibidas nesta seção, incluindo a adição e remoção de chaves de licença.
- Você não pode criar pacotes de instalação personalizados.
- Você não pode criar funções personalizadas para usuários.

- O recurso Ataque de vírus não está disponível. Os eventos Ataques de vírus não são armazenados e nenhuma notificação é enviada.
- O repositório **Objetos excluídos** não está disponível.
- Você não pode ativar a adição de eventos em lote (aqueles publicados em grandes quantidades) ao banco de dados.
- A migração de Servidores de Administração do modo no local para o modo Cloud Console não é suportada.
- As informações estatísticas da KSN dos componentes do Servidor de Administração, como o Servidor de Administração ou o Agente de Rede, não são enviadas para a Kaspersky.

Alguns limites também são impostos na criação de determinados objetos do aplicativo (veja a tabela abaixo). Se qualquer destes limites for excedido quando for feita uma tentativa de criar tal objeto, a criação do objeto será bloqueada e uma mensagem de erro sobre o limite será exibida.

Limitações na criação de objetos do Kaspersky Security Center Cloud Console no modo de avaliação

Tipo de limitação	Valor
Políticas	8
Tarefas	17
Chaves de licença	1
Pacotes de instalação	5
Seleções de dispositivos (instâncias predefinidas não incluídas)	5
Seleções de eventos (instâncias predefinidas não incluídas)	5
Regras de migração de dispositivos	3
Modelos de relatório do mesmo tipo	10
Grupos de segurança internos	20
Dispositivos gerenciados	20

Usando o Kaspersky Marketplace para escolher as soluções comerciais Kaspersky de sua preferência

Marketplace é uma seção no menu principal que permite visualizar toda a gama de soluções comerciais Kaspersky. Selecione as que você precisa e prossiga com a compra no site da Kaspersky. Você pode usar filtros para visualizar apenas as soluções que se adaptam à sua organização e aos requisitos do seu sistema de segurança da informação. Ao selecionar uma solução, o Kaspersky Security Center Cloud Console redireciona o acesso para a página da web no site da Kaspersky com mais informações sobre a solução. Cada página da web permite efetuar compra ou contém instruções sobre o processo de compra.

Na seção **Marketplace**, você pode filtrar as soluções Kaspersky usando os seguintes critérios:

- Número de dispositivos (endpoints, servidores e outros tipos de ativos) que você deseja proteger:
  - 50–250
  - 250–1000

- Mais de 1000

- Nível de experiência da equipe de segurança da informação da sua organização:

  - **Foundations**

    Este nível é típico para empresas que possuem apenas uma equipe de TI. O número máximo possível de ameaças é bloqueado automaticamente.

  - **Optimum**

    Esse nível é típico para empresas que têm uma função de segurança de TI específica na equipe de TI. Nesse nível, as empresas precisam de soluções que lhes permitam enfrentar as ameaças genéricas e também as que desviam dos mecanismos preventivos existentes.

  - **Expert**

    Este nível é típico para empresas com ambientes de TI complexos e distribuídos. A equipe de segurança de TI é experiente ou a empresa possui uma equipe de SOC (Security Operations Center). As soluções necessárias permitem que as empresas enfrentem ameaças complexas e ataques direcionados.

- Tipos de ativos que você deseja proteger:

  - **Endpoints**: estações de trabalho de funcionários, máquinas físicas e virtuais, sistemas integrados

  - **Servidores**: servidores físicos e virtuais

  - **Nuvem**: ambientes de nuvem pública, privada ou híbrida; serviços na nuvem

  - **Rede**: rede local, infraestrutura de TI

  - **Serviço**: serviços relacionados à segurança fornecidos pela Kaspersky

Para encontrar e adquirir uma solução empresarial Kaspersky:

1. No menu principal, vá para **Marketplace**.

   Por padrão, a seção exibe todas as soluções comerciais Kaspersky disponíveis.

2. Para visualizar apenas as soluções adequadas à sua organização, selecione os valores necessários nos filtros.

3. Clique na solução que deseja adquirir ou sobre a qual deseja saber mais.

   Você será redirecionado para a página da solução. Você pode seguir as instruções na tela para prosseguir com a compra.

Licenças e quantidade mínima de dispositivos para cada licença

Caso deseje usar o Kaspersky Security Center Cloud Console no modo comercial, será necessário adquirir uma licença antes de criar seu primeiro espaço de trabalho. A tabela abaixo exibe as licenças que você pode adquirir e a quantidade mínima de dispositivos para cada licença (mesmo se desejar proteger menos dispositivos):

Licenças que permitem o uso do Kaspersky Security Center Cloud Console

Licença	Quantidade mínima de dispositivos (mesmo que você deseje proteger uma quantidade menor)

Kaspersky Endpoint Security for Business Select	Para licenças comerciais: 300 Para licenças comerciais (assinatura): 100
Kaspersky Endpoint Security for Business Advanced	Para licenças comerciais: 300 Para licenças comerciais (assinatura): 100
Kaspersky Total Security for Business	300
Kaspersky Endpoint Detection and Response Optimum	Para licenças comerciais: 300 Para licenças comerciais (assinatura): 100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Hybrid Cloud Security, Desktop	Para licenças comerciais: 300 Para licenças comerciais (assinatura): 100
Kaspersky Hybrid Cloud Security, Servidor	50
Kaspersky Hybrid Cloud Security, Core	20
Kaspersky Hybrid Cloud Security, CPU	20
Kaspersky Hybrid Cloud Security Enterprise, Desktop	Para licenças comerciais: 300 Para licenças comerciais (assinatura): 100
Kaspersky Hybrid Cloud Security Enterprise, Servidor	50
Kaspersky Hybrid Cloud Security Enterprise, CPU	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security Compliance Edition	300
Kaspersky Symphony (disponível apenas na Rússia atualmente)	300
Kaspersky Next EDR Foundations	300 usuários (cada licença de usuário pode ser aplicada a 1 dispositivo PC/Mac e a 2 dispositivos móveis)
Kaspersky Next EDR Optimum	300 usuários (cada licença de usuário pode ser aplicada a 1 dispositivo PC/Mac e a 2 dispositivos móveis)
Kaspersky Next XDR Expert	250 usuários (cada licença de usuário pode ser aplicada a 1 dispositivo PC/Mac e 2 dispositivos móveis)

O máximo de dispositivos por um espaço de trabalho é 25.000. Caso queira proteger mais de 10.000 dispositivos, é necessário criar um espaço de trabalho separado. Para isso, envie uma solicitação ao Suporte Técnico da Kaspersky. A solicitação deve conter as seguintes informações:

- **E-mail do usuário** – o endereço de e-mail do usuário registrado no Kaspersky Security Center Cloud Console. Esse usuário recebe direitos de administrador no espaço de trabalho criado.

  Depois de criar uma conta no Kaspersky Security Center Cloud Console, não é preciso registrar uma empresa e criar um espaço de trabalho para ela. Especifique as informações sobre a empresa e o espaço de trabalho na solicitação.

- **Nome da empresa** – o nome da empresa na qual deseja usar o Kaspersky Security Center Cloud Console.
- **País da empresa** – o país no qual a empresa está localizada.
- **Nome do espaço de trabalho** – o nome do espaço de trabalho a ser criado para a empresa.
- **Contagem estimada de endpoints** – o número total de dispositivos cliente (incluindo dispositivos móveis) que deseja proteger no novo espaço de trabalho.
- **País do espaço de trabalho** – o país no qual deseja localizar o novo espaço de trabalho. Esse parâmetro afeta a seleção do data center para armazenar o espaço de trabalho.

  Observe que, se desejar localizar o espaço de trabalho nos Estados Unidos ou Canadá, especifique o estado ou a província para determinar a região do data center.

  Os parâmetros **País da empresa** e **País do espaço de trabalho** podem ser iguais.
- **Código de ativação** – o código de ativação recebido depois de comprar o Kaspersky Security Center Cloud Console. Certifique-se de que a licença que deseja comprar abrange todos os dispositivos clientes que devem ser protegidos.

Após o envio da solicitação, os especialistas da Kaspersky registram a empresa especificada e criam um espaço de trabalho para ela. Quando a criação do espaço de trabalho for concluída, será enviada uma notificação por e-mail para o usuário. É possível fazer login em sua conta no Kaspersky Security Center Cloud Console para visualizar o resultado.

Eventos do limite do licenciamento excedidos

O Kaspersky Security Center Cloud Console permite obter informações sobre eventos quando alguns limites de licenciamento são excedidos pelos aplicativos Kaspersky instalados nos dispositivos cliente.

O nível de importância de tais eventos quando uma restrição de licenciamento for excedida é definido de acordo com as seguintes regras:

- Se o número de unidades atualmente usadas cobertas por uma única licença estiver entre 90% e 100% do número total de unidades cobertas pela licença, o evento é publicado com o nível de importância **Informação**.
- Se o número de unidades atualmente usadas cobertas por uma única licença estiver entre 100% e 110% do número total de unidades cobertas pela licença, o evento é publicado com o nível de importância **Aviso**.
- Se o número de unidades atualmente usadas cobertas por uma licença exceder 110% do número total de unidades cobertas pela mesma licença, o evento será publicado com o nível de importância de **Evento crítico**.

Métodos de distribuição dos códigos de ativação para os dispositivos gerenciados

Os aplicativos da Kaspersky instalados em dispositivos gerenciados devem ser licenciados ao aplicar um código de ativação para cada um dos aplicativos. Não é possível usar arquivos de chave para o licenciamento de aplicativos gerenciados; somente códigos de ativação são aceitos. Um código de ativação pode ser implementado nas seguintes formas:

- Implementação automática

- A tarefa de adicionar uma chave de licença para um aplicativo gerenciado
- Ativação manual de um aplicativo gerenciado

Os aplicativos Kaspersky podem usar mais de uma chave de licença ao mesmo tempo. Por exemplo, o Kaspersky Endpoint Security for Windows pode usar duas chaves de licença: uma para Kaspersky Endpoint Security for Windows e outra para ativação das funções integradas do Endpoint Detection and Response.

Além disso, os aplicativos Kaspersky podem ter não apenas uma chave de licença ativa, mas também uma chave de licença adicional. Um aplicativo da Kaspersky usa uma chave ativa no momento e armazena uma chave reserva para aplicar após a expiração da chave ativa. É possível adicionar uma nova chave de licença ativa ou reserva por qualquer um dos métodos listados acima. O aplicativo ao qual a chave de licença é adicionada define se a chave é ativa ou reserva. A definição da chave não depende do método usado para adicionar uma nova chave de licença.

Adição de uma chave de licença ao repositório do Servidor de Administração

Ao adicionar uma chave de licença usando o Kaspersky Security Center Cloud Console, as configurações da chave de licença são salvas no Servidor de Administração. Com base nestas informações, o aplicativo gera um relatório sobre o uso das chaves de licença e notifica o administrador sobre a expiração das licenças e sobre a violação das restrições de licença que estão definidas nas propriedades das chaves de licença. Você pode configurar as notificações do uso de chaves de licença dentro das configurações do Servidor de Administração.

Adicionar uma chave de licença ao repositório do Servidor de Administração:

1. No menu principal, vá para **Operações → Licenciamento → Licenças da Kaspersky**.
2. Clique no botão **Adicionar**.
3. Especifique o código de ativação no campo de texto e clique no botão **Enviar**.
4. Clique no botão **Fechar**.

A chave de licença ou várias chaves de licença são adicionadas ao repositório do Servidor de Administração.

Implementando uma chave de licença para dispositivos cliente

O Kaspersky Security Center Cloud Console permite distribuir uma chave de licença para dispositivos clientes automaticamente ou com o uso da tarefa de adição de chaves.

Antes da implementação, adicione uma chave de licença ao repositório do Servidor de Administração.

Para distribuir uma chave de licença para dispositivos clientes usando a tarefa de adição de chaves:

1. No menu principal, vá para **Ativos (dispositivos) → Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para Novas Tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na lista suspensa **Aplicativo**, selecione o aplicativo ao qual você deseja adicionar uma chave de licença.
4. Na lista **Tipo de tarefa**, selecione a tarefa de **Adicionar chave**.
5. No campo **Nome da tarefa**, especifique o nome da nova tarefa.
6. Selecione os dispositivos aos quais a tarefa será atribuída.
7. Na etapa **Selecionando uma chave de licença** do assistente, clique no link **Adicionar chave** para adicionar a chave.
8. No painel de adição de chave, adicione a chave de licença usando uma das seguintes opções:

   Adicione a chave de licença somente se não a tiver adicionado no repositório do Servidor de Administração antes de criar a tarefa de adição de chave.

   - Selecione a opção **Insira o código de ativação** para inserir um código de ativação e, então, faça o seguinte:

     a. Especifique o código de ativação e, então, clique no botão **Enviar**.

     As informações sobre a chave de licença são exibidas no painel de adição de chave.

     b. Clique no botão **Salvar**.

     Se você quiser distribuir automaticamente a chave de licença para dispositivos gerenciados, ative a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

     O painel de adição de chave é fechado.

   - Selecione a opção **Adicionar arquivo de chave** para adicionar um arquivo de chave e, em seguida:

     a. Clique no botão **Selecionar arquivo de chave**.

     b. Na janela exibida, selecione um arquivo de chave e, então, clique no botão **Abrir**.

     As informações sobre a chave de licença são exibidas no painel de adição de chave de licença.

     c. Clique no botão **Salvar**.

     Se você quiser distribuir automaticamente a chave de licença para dispositivos gerenciados, ative a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

     O painel de adição de chave é fechado.
9. Selecione a chave de licença na tabela de chaves.
10. Na etapa **Informações da licença** do assistente, ative a opção **Usar como chave reserva** para usar essa chave como reserva.

    Neste caso, a chave reserva é aplicada após a expiração da chave ativa.
11. Na etapa **Concluir a criação da tarefa** do assistente, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** para modificar as configurações padrão da tarefa.

Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois.

12. Clique no botão **Concluir**.

    O assistente cria a tarefa. Se você ativou a opção **Abrir detalhes da tarefa quando a criação for concluída**, a janela de propriedades da tarefa abre automaticamente. Nesta janela, você pode especificar as configurações gerais da tarefa e, se necessário, alterar as configurações especificadas durante a criação da tarefa.

    > Você também pode abrir a respectiva janela de propriedades clicando no nome da tarefa criada na lista de tarefas.

    A tarefa é criada, configurada e exibida na lista de tarefas.

13. Para executar a tarefa, selecione-a na lista de tarefas e, então, clique no botão **Iniciar**.

    Você também pode definir um agendamento de início de tarefa na guia **Agendamento** da janela de propriedades da tarefa.

    Para obter uma descrição detalhada das configurações de início agendado, consulte as configurações gerais da tarefa.

Depois que a tarefa for concluída, a chave de licença será implementada nos dispositivos selecionados.

Distribuição automática de uma chave de licença

O Kaspersky Security Center Cloud Console permite a distribuição automática de chaves de licença para os dispositivos gerenciados, se elas estiverem localizadas no repositório de chaves de licença do Servidor de Administração.

Para distribuir automaticamente uma chave de licença para os dispositivos gerenciados:

1. No menu principal, vá para **Operações** → **Licenciamento** → **Licenças da Kaspersky**.
2. Clique em o nome da chave de licença que você pretende distribuir automaticamente para os dispositivos.
3. Na janela de propriedades da chave de licença que é aberta, alterne para **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.
4. Clique no botão **Salvar**.

A chave de licença será distribuída automaticamente para todos os dispositivos compatíveis.

A distribuição de chaves de licença é realizada através do Agente de Rede. Não é criada nenhuma tarefa de distribuição de chaves de licença para o aplicativo.

Durante a distribuição automática de uma chave de licença, o limite de licenciamento no número de dispositivos é levado em conta. O limite de licenciamento é definido nas propriedades da chave de licença. Se o limite de licenciamento for alcançado, a distribuição desta chave de licença nos dispositivos termina automaticamente.

Observe que uma chave de licença distribuída automaticamente pode não ser exibida no repositório do Servidor de Administração virtual nos seguintes casos:

- A chave de licença não é válida para o aplicativo.

- O Servidor de Administração virtual não tem dispositivos gerenciados.
- A chave de licença já foi usada para dispositivos gerenciados por outro Servidor de Administração virtual e o limite no número de dispositivos foi atingido.

Se você especificar a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados** de uma chave de licença de assinatura para ativar qualquer aplicativo em um dispositivo gerenciado e, ao mesmo tempo, tiver uma chave de licença de teste ativa, a chave de licença de teste será automaticamente substituída pela chave de licença de assinatura oito dias antes da data de expiração.

Visualizando informações sobre as chaves de licença em uso no repositório do Servidor de Administração

Para exibir a lista das chaves de licença adicionadas ao repositório do Servidor de Administração,

No menu principal, vá para **Operações → Licenciamento → Licenças da Kaspersky**.

A lista exibida contém códigos de ativação adicionados ao repositório do Servidor de Administração.

Para exibir as informações detalhadas sobre uma chave de licença:

1. No menu principal, vá para **Operações → Licenciamento → Licenças da Kaspersky**.
2. Clique no nome da chave de licença necessária.

Na janela de propriedades da chave de licença que se abre, você pode visualizar:

- Na guia **Geral**: as informações principais sobre a chave de licença
- Na guia **Dispositivos**: a lista de dispositivos cliente em que a chave de licença foi usada para a ativação do aplicativo da Kaspersky instalado

Visualizando informações sobre as chaves de licença usadas para um aplicativo Kaspersky específico

Para saber quais chaves de licença estão em uso para um aplicativo da Kaspersky:

1. No menu principal, vá para **Ativos (dispositivos) → Dispositivos gerenciados**.

   Se o dispositivo pertencer ao grupo de Dispositivos não atribuídos, acesse **Descoberta e implementação → Dispositivos não atribuídos**, em vez disso.
2. Clique no nome do dispositivo necessário.
3. Na janela de propriedades do dispositivo que será aberta, selecione a seção **Aplicativos**.
4. Na lista de aplicativos aberta, selecione o aplicativo cujas chaves de licença você deseja visualizar.
5. Na janela de propriedades do aplicativo aberta, na guia **Geral**, selecione a seção **chaves de licença**.

As informações são exibidas no espaço de trabalho desta seção.

Excluindo uma chave de licença do repositório

É possível excluir uma chave de licença do repositório do Servidor de Administração. Observe que o Kaspersky Security Center Cloud Console exclui automaticamente o espaço de trabalho após 90 dias nos seguintes casos:

- O usuário exclui a última chave de licença (ativa, reserva ou não em uso) adicionada manualmente no repositório.
- A última chave de licença expira.

Caso o espaço de trabalho seja excluído, não será possível gerenciar a proteção da rede por meio do Kaspersky Security Center Cloud Console. O usuário também perde permanentemente os dados do Kaspersky Security Center Cloud Console. Caso necessário, também é possível excluir o espaço de trabalho manualmente. Caso contrário, recomendamos manter pelo menos uma chave de licença no repositório do Servidor de Administração.

Caso uma chave de licença seja excluída e uma chave reserva de licença tenha sido adicionada anteriormente, a chave reserva de licença se tornará automaticamente a chave de licença ativa após a exclusão ou expiração da chave ativa anterior.

Se você excluir a chave de licença ativa implementada em um dispositivo gerenciado, o aplicativo continuará funcionando no dispositivo gerenciado.

Para excluir uma chave de licença do repositório do Servidor de Administração:

1. Verifique se o Servidor de Administração não usa uma chave de licença que se deseja excluir. Caso o Servidor de Administração use a chave, não será possível excluí-la. Para realizar a verificação:

   a. No menu principal, clique no ícone de configurações () ao lado do Servidor de Administração.

      A janela Propriedades do Servidor de Administração é aberta.

   b. Na guia **Geral**, selecione a seção **Chaves de licença**.

   c. Caso a chave de licença seja exibida na seção aberta, clique no botão **Remover chave de licença ativa** e, em seguida, confirme a operação. Depois disso, o Servidor de Administração não usa a chave de licença excluída, mas a chave permanece no repositório do Servidor de Administração. Caso a chave de licença necessária não seja exibida, o Servidor de Administração não a utilizará.

2. No menu principal, vá para **Operações → Licenciamento → Licenças da Kaspersky**.

3. Selecione a chave de licença necessária e clique no botão **Excluir**.

4. Na janela aberta, marque a caixa de seleção **Entendo os riscos e desejo excluir a chave de licença**. Isso significa que, se a última chave de licença for excluída, o usuário está ciente da exclusão subsequente do espaço de trabalho e da perda de controle sobre os dispositivos gerenciados. Em seguida, clique no botão **Excluir**.

Como resultado, a chave de licença selecionada é excluída do repositório.

É possível adicionar novamente uma chave de licença excluída ou adicionar uma nova chave de licença. Caso tenha excluído a última chave de licença, também será possível adicionar uma chave de licença, desde que o espaço de trabalho não tenha sido excluído. O Kaspersky Security Center Cloud Console notifica os administradores do espaço de trabalho 30 dias, 7 dias e 1 dia antes de exclusão.

Visualizar a lista de dispositivos em que um aplicativo da Kaspersky não está ativado

É possível visualizar a lista de todos os dispositivos nos quais um aplicativo da Kaspersky está instalado, mas não ativado (por exemplo, a licença está ausente ou expirou).

Para visualizar os dispositivos nos quais um aplicativo Kaspersky não está ativado:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.

   A lista de tarefas é exibida.

2. Clique no nome da tarefa de Atualização relacionada ao aplicativo da Kaspersky em questão.

   A janela de propriedades da tarefa é exibida com várias guias nomeadas.

3. Na janela de propriedades da tarefa, selecione a seção **Resultados**.

   Na coluna **Dispositivo**, são exibidos os dispositivos nos quais a tarefa foi bem-sucedida.

4. Classifique a coluna **Dispositivo**.

   Na coluna **Dispositivo**, são exibidos os dispositivos nos quais a tarefa foi bem-sucedida. Os dispositivos em que a tarefa falhou devido à ausência de uma licença são dispositivos em que o aplicativo não está ativado.

Revogando o consentimento com um Contrato de Licença do Usuário Final

Se você decidir parar de proteger alguns de seus dispositivos clientes, poderá revogar o Contrato de Licença do Usuário Final (EULA) para qualquer aplicativo da Kaspersky gerenciado. Você deve desinstalar o aplicativo selecionado e seus pacotes de instalação antes de revogar o EULA. Os pacotes de instalação devem ser excluídos do Servidor de Administração e dos Servidores de Administração virtuais.

Os EULAs aceitos em um Servidor de Administração virtual podem ser revogados no Servidor de Administração virtual ou no Servidor de Administração principal. Os EULAs aceitos em um Servidor de Administração principal podem ser revogados somente no Servidor de Administração principal.

Para revogar o EULA dos aplicativos gerenciados da Kaspersky:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral** da janela do Servidor de Administração, selecione a seção **Contratos de Licença do Usuário Final**.

   Uma lista de EULAs, aceitos ao criar pacotes de instalação ou durante a instalação contínua de atualizações, é exibida.

3. Na lista, selecione o EULA que deseja revogar.

   Você pode visualizar as seguintes propriedades da EULA:

   - Data em que o EULA foi aceito

- Nome do usuário que aceitou o EULA
- Se o EULA pode ou não ser revogado

4. Clique na data de aceite de qualquer EULA para abrir sua janela de propriedades que exibe os seguintes dados:
   - Nome do usuário que aceitou o EULA
   - Data em que o EULA foi aceito
   - Identificador exclusivo (UID) do EULA
   - Texto completo do EULA
   - Lista de objetos (pacotes de instalação, atualizações contínuas) vinculados ao EULA e seus respectivos nomes e tipos
5. Na parte inferior da janela de propriedades do EULA, clique no botão **Revogar Contrato de Licença**.

   Se o EULA selecionado puder ser revogado apenas desinstalando o aplicativo ou apenas no Servidor de Administração principal, uma notificação sobre esta restrição será exibida, em vez do botão **Revogar Contrato de Licença**.

   > Se existirem objetos (pacotes de instalação e suas respectivas tarefas) que impeçam a revogação do EULA, será exibida uma notificação. Não é possível continuar com a revogação até que esses objetos sejam excluídos.

   Na janela que se abre, você é informado que deve primeiro desinstalar o aplicativo da Kaspersky que corresponde ao EULA.
6. Clique no botão para confirmar a revogação.

A EULA foi revogada. Ele não é mais exibido na lista de Contratos de licença na seção **Contratos de Licença do Usuário Final**. A janela de propriedades do EULA se fecha; o aplicativo não estará mais instalado.

Renovando licenças para aplicativos da Kaspersky

Você pode renovar uma licença de um aplicativo da Kaspersky que expirou ou está prestes a expirar (em menos de 30 dias).

> Caso a última chave de licença tenha expirado, o Kaspersky Security Center Cloud Console excluirá automaticamente o espaço de trabalho após 90 dias. Assim, não será possível gerenciar a proteção da rede por meio do Kaspersky Security Center Cloud Console. O usuário também perde permanentemente os dados do Kaspersky Security Center Cloud Console. Recomendamos renovar as chaves de licença desatualizadas ou adicionar novas chaves no repositório do Servidor de Administração para manter o espaço de trabalho.

Para ver uma notificação sobre uma licença expirada ou uma licença que está prestes a expirar:

1. Execute alguma das seguintes ações:
   - No menu principal, vá para **Operações → Licenciamento → Licenças da Kaspersky**.

- No menu principal, vá para **Monitoramento e relatórios** → **Painel**, e depois clique no link **Ver licenças prestes a expirar** ao lado de uma notificação.

A janela **Licenças da Kaspersky** é aberta e você pode ver e renovar as licenças prestes a expirar e expiradas.

2. Se deseja renovar uma licença, clique no link **Renovar licença** ao lado da licença necessária.

   Ao clicar em um link de renovação de licença, você concorda em transferir os seguintes dados para a Kaspersky: ID do software, versão do software, localização do software, ID da licença e um atributo que mostra se a licença foi fornecida por uma empresa parceira. Os dados são necessários para determinar os termos de renovação de sua licença.

3. Na janela aberta do serviço de renovação de licença, siga as instruções para renovar uma licença.

   A licença expirada é renovada.

No Kaspersky Security Center Cloud Console, são exibidas notificações quando uma licença está prestes a expirar, de acordo com a seguinte programação:

- 30 dias antes do vencimento
- 7 dias antes do vencimento
- 3 dias antes do vencimento
- 24 horas antes do vencimento
- Quando uma licença expirou

Uso do Kaspersky Security Center Cloud Console após a expiração da licença

Após a expiração da licença, a Kaspersky pode conceder a você o uso do Kaspersky Security Center Cloud Console por até 90 dias, sem limitações. Durante esse período, o Servidor de Administração, o Agente de Rede e a interface da Web do Kaspersky Security Center Cloud Console funcionam sem limitações. O Kaspersky Security Center Cloud Console também envia estatísticas da KSN para a Kaspersky de acordo com as configurações atuais de acesso da KSN. Os aplicativos gerenciados funcionam apenas com funcionalidade limitada (para obter detalhes, consulte a documentação de tais aplicativos).

Quando a licença tiver expirado há 90 dias, o Kaspersky Security Center Cloud Console exclui automaticamente o espaço de trabalho. Caso queira manter o espaço de trabalho, renove pelo menos uma chave de licença expirada ou adicione uma nova ao repositório.

Kaspersky Security Network (KSN)

Essa seção descreve como usar uma infraestrutura de serviços on-line, denominada Kaspersky Security Network (KSN). A seção fornece os detalhes sobre a KSN, assim como instruções sobre como ativar a KSN, configurar o acesso à KSN e visualizar as estatísticas sobre o uso do Servidor proxy da KSN.

Sobre a KSN

A Kaspersky Security Network (KSN) é uma infraestrutura de serviços on-line que fornece o acesso à Base de Dados de Conhecimento on-line da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software. O uso de dados a partir da Kaspersky Security Network garante uma resposta mais rápida dos aplicativos Kaspersky a ameaças, melhora a efetividade de alguns componentes de proteção e reduz o risco de falsos positivos. A KSN permite usar os bancos de dados de reputação da Kaspersky para obter informações sobre os aplicativos instalados nos dispositivos cliente.

Caso participe da KSN, você concorda em enviar informações à Kaspersky, no modo automático, as informações sobre a operação dos aplicativos Kaspersky instalados nos dispositivos cliente gerenciados pelo Kaspersky Security Center Cloud Console. As informações são transferidas de acordo com as configurações de acesso da KSN atuais. Os analistas da Kaspersky também averiguam as informações recebidas e as incluem nos bancos de dados estatísticos e de reputação da Kaspersky Security Network.

O aplicativo solicita a participação da KSN durante a execução do Assistente de início rápido. É possível iniciar ou parar de usar a KSN a qualquer momento durante o uso do aplicativo.

Você usa o KSN de acordo com a Declaração KSN lida e aceita ao ativar a KSN. Se a Declaração KSN for atualizada, a nova versão será exibida ao atualizar ou fazer upgrade do Servidor de Administração. Você pode aceitar a Declaração KSN atualizada ou recusá-la. Se recusar, continuará usando a KSN de acordo com a versão Declaração KSN aceita anteriormente.

Quando a KSN está ativada, o Kaspersky Security Center Cloud Console verifica se os servidores da KSN estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos. Isso é necessário para garantir que o nível de segurança seja mantido para os dispositivos gerenciados.

Os dispositivos cliente gerenciados pelo Servidor de Administração interagem com a KSN por meio do servidor proxy da KSN. O servidor proxy da KSN fornece os seguintes recursos:

- Os dispositivos cliente podem enviar solicitações à KSN e transferir informações para a KSN mesmo que não tenham acesso direto à Internet.
- O servidor proxy KSN armazena em cache os dados processados, o que reduz a carga de trabalho no canal de saída e o período de tempo despendido para aguardar por informações solicitadas por um dispositivo cliente.

Você pode ativar o servidor proxy da KSN no lado do ponto de distribuição para fazer o dispositivo funcionar como um servidor proxy da KSN. Neste caso, o serviço de Proxy da KSN (ksnproxy) é executado no dispositivo.

Ativar e desativar a KSN

Para ativar a KSN:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações do KSN**.

3. Alterne o botão para a posição **Usar a Kaspersky Security Network Ativado**.

   A KSN está ativada.

Se o botão de alternância estiver ativado, os dispositivos cliente enviarão os resultados da instalação de patches para a Kaspersky. Ao ativar este botão de alternância, você deve ler e aceitar os termos da Declaração da KSN.

4. Clique no botão **Salvar**.

Para desativar a KSN:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações do KSN**.

3. Alterne o botão para a posição **Usar a Kaspersky Security Network Desativado**.

   A KSN está desativada.

   Se o botão de alternância estiver desativado, os dispositivos cliente não enviarão resultados da instalação de patches para a Kaspersky.

4. Clique no botão **Salvar**.

Visualizando a Declaração da KSN aceita

Ao ativar o Kaspersky Security Network (KSN), você deve ler e aceitar a Declaração da KSN. Você pode ver a Declaração da KSN aceita a qualquer momento.

Para visualizar a declaração KSN aceita:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações de KSN**.

3. Clique no link **Ver Declaração sobre coleta de dados da KSN**.

Na janela aberta, você pode ver o texto da Declaração KSN aceita.

Aceitando uma declaração da KSN atualizada

Você usa o KSN de acordo com a Declaração KSN lida e aceita ao ativar a KSN. Se a Declaração da KSN for atualizada, ela será exibida automaticamente ao abrir o Kaspersky Security Center Cloud Console. Você pode aceitar a Declaração KSN atualizada ou recusá-la. Caso a declaração seja recusada, o usuário continuará usando a KSN de acordo com a versão Declaração da KSN aceita anteriormente. É possível visualizar e aceitar a Declaração da KSN atualizada posteriormente.

Para visualizar e aceitar ou recusar uma Declaração da KSN atualizada:

1. Clique no link **Exibir notificações** no canto superior direito da janela do aplicativo principal.

   A janela **Notificações** se abre.

2. Clique no link **Ver a Declaração da KSN atualizada**.

A janela **Atualização da Declaração da Kaspersky Security Network** se abre.

3. Leia a Declaração da KSN e, em seguida, decida-se clicando em um dos seguintes botões:

   - **Eu aceito a declaração da KSN atualizada**
   - **Usar KSN sob as condições da Declaração anterior**

   Dependendo da sua escolha, a KSN continuará funcionando de acordo com os termos da Declaração da KSN em vigor ou atualizada. Você pode ver o texto da Declaração da KSN aceita nas propriedades do Servidor de Administração a qualquer momento.

Verificar se o ponto de distribuição funciona como servidor proxy da KSN

Em um dispositivo gerenciado atribuído como ponto de distribuição é possível ativar o servidor proxy da KSN. Um dispositivo gerenciado funciona como servidor proxy da KSN quando o serviço ksnproxy está sendo executado no dispositivo. É possível verificar, ativar ou desativar esse serviço localmente no dispositivo.

Você pode atribuir um dispositivo baseado em Windows ou Linux como um ponto de distribuição. O método de verificação do ponto de distribuição depende de seu sistema operacional.

Para verificar se o ponto de distribuição baseado em Windows funciona como servidor proxy da KSN:

1. No dispositivo de ponto de distribuição, no Windows, abra **Serviços** (**Todos os programas** → **Ferramentas administrativas** → **Serviços**).

2. Na lista de serviços, verifique se o serviço ksnproxy está sendo executado.

   Se o serviço ksnproxy estiver em execução, o Agente de Rede do dispositivo participa da Kaspersky Security Network e funciona como servidor proxy da KSN para os dispositivos gerenciados incluídos no escopo do ponto de distribuição.

Se desejar, você pode desativar o serviço ksnproxy. Nesse caso, o Agente de Rede no ponto de distribuição para de participar da Kaspersky Security Network. Isso requer direitos de administrador local.

Para verificar se o ponto de distribuição baseado em Linux funciona como servidor proxy da KSN:

1. No dispositivo do ponto de distribuição, exiba a lista de processos em execução.

2. Na lista de processos em execução, verifique se o processo `/opt/kaspersky/ksc64/sbin/ksnproxy` está em execução.

Caso o processo `/opt/kaspersky/ksc64/sbin/ksnproxy` esteja em execução, o Agente de Rede do dispositivo participa da Kaspersky Security Network e funciona como servidor proxy da KSN para os dispositivos gerenciados incluídos no escopo do ponto de distribuição.

Definições de licenciamento

Esta seção apresenta definições sobre o licenciamento de aplicativos Kaspersky gerenciados pelo Kaspersky Security Center Cloud Console.

Sobre a licença

Uma *licença* é um direito com período de validade limitado para uso do Kaspersky Security Center Cloud Console, concedido nos termos do Contrato de Licença (Contrato de Licença de Usuário Final).

O escopo dos serviços e o período de validade dependem da licença sob a qual o aplicativo é utilizado.

São fornecidos os seguintes tipos de licença:

- *Avaliação*

  Uma licença gratuita concebida para experimentar o aplicativo. Uma licença de avaliação normalmente tem um prazo de validade curto.

  Quando uma licença de avaliação expira, todos os recursos do Kaspersky Security Center Cloud Console são desativados. Para continuar usando o aplicativo, é necessário comprar a licença comercial.

  Você pode usar o aplicativo com uma licença de avaliação por apenas um período de avaliação.

- *Comercial*

  Uma licença paga.

  Quando uma licença comercial expira, os principais recursos do aplicativo são desativados. Para continuar usando o Kaspersky Security Center Cloud Console, é necessário renovar sua licença. Após a expiração de uma licença comercial, não é possível continuar usando o aplicativo e ele deve ser removido do dispositivo.

  Recomendamos a renovação da sua licença antes que ela expire para garantir a máxima proteção contra todas as ameaças à segurança.

Sobre o certificado de licença

O *Certificado de licença* é um documento que você recebe juntamente com um arquivo de chave ou um código de ativação.

Um certificado de licença contém as seguintes informações sobre a licença fornecida:

- Chave de licença ou número do pedido
- Informações sobre o usuário ao qual foi concedida a licença
- Informações sobre o aplicativo que pode ser ativado com a licença fornecida
- Limite do número de unidades de licenciamento (por exemplo, dispositivos nos quais o aplicativo pode ser usado com uma licença fornecida)
- Data de início da validade da licença
- Data de expiração da licença ou período da licença
- Tipo de licença

Sobre a chave de licença

Chave de licença é a sequência de bits que você pode aplicar para ativar e usar o aplicativo de acordo com os termos do Contrato de Licença do Usuário Final. As chaves de licença são geradas pelos especialistas da Kaspersky.

É possível adicionar uma chave de licença ao aplicativo inserindo um *código de ativação*. A chave de licença é exibida na interface do aplicativo como uma sequência alfanumérica única após você a adicionar ao aplicativo.

A chave de licença pode estar bloqueada pela Kaspersky caso os termos do Contrato de Licença tenham sido violados. Se a chave de licença tiver sido bloqueada, você deve adicionar outra se desejar usar o aplicativo.

Uma chave de licença pode ser ativa ou adicional (ou reserva).

Uma *chave de licença ativa* é uma chave de licença que é atualmente usada pelo aplicativo. Uma chave de licença ativa pode ser adicionada para uma licença de avaliação ou comercial. O aplicativo não pode ter mais de uma chave de licença ativa.

Uma *chave de licença adicional (ou reserva)* é uma chave de licença que permite ao usuário utilizar o aplicativo, mas que não se encontra atualmente em uso. A chave de licença adicional torna-se automaticamente ativa quando a licença associada à chave atual expira. Uma chave de licença adicional pode ser adicionada somente se uma chave de licença atual tiver sido adicionada.

Uma chave de licença para uma licença de avaliação pode ser adicionada somente como um chave de licença atual. Uma chave de licença para uma licença de avaliação não pode ser adicionada como uma chave de licença adicional.

Sobre o código de ativação

Código de ativação é uma sequência única de 20 caracteres alfanuméricos. Você insere um código de ativação para adicionar uma chave de licença que ativa o Kaspersky Security Center Cloud Console. Você recebe o código de ativação através do endereço de e-mail que você especificou, após comprar o Kaspersky Security Center Cloud Console ou após fazer o pedido da versão de avaliação do Kaspersky Security Center Cloud Console.

Para ativar o aplicativo com um código de ativação, é necessário acesso à Internet para estabelecer a conexão com os servidores de ativação da Kaspersky. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos.

Se o aplicativo foi ativado com um código de ativação, o aplicativo em alguns casos envia solicitações regulares aos servidores de ativação da Kaspersky para verificar o status atual da chave de licença. Você precisa de fornecer o acesso à Internet ao aplicativo para ser possível enviar solicitações.

Se você perdeu seu código de ativação após instalar o aplicativo, entre em contato com o parceiro da Kaspersky do qual você comprou a licença.

Não é possível usar arquivos de chave para ativar aplicativos gerenciados; somente códigos de ativação são aceitos.

Sobre a assinatura

A *Assinatura para o Kaspersky Security Center Cloud Console* é um pedido para uso do aplicativo sob as configurações selecionadas (data de expiração da assinatura, número de dispositivos protegidos). Você pode registrar sua assinatura do Kaspersky Security Center Cloud Console com seu provedor de serviços (por exemplo, seu provedor de Internet). Uma assinatura pode ser renovada manualmente ou no modo automático; você também pode cancelá-la.

Uma assinatura pode ser limitada (por exemplo, um ano) ou ilimitada (sem uma data de expiração). Para continuar a usar o Kaspersky Security Center Cloud Console após uma assinatura limitada expirar, você precisa renová-la. Uma assinatura ilimitada é automaticamente renovada, caso tenha sido pré-paga ao provedor de serviços nas datas devidas.

Quando uma assinatura limitada expirar, um período adicional poderá lhe ser fornecido para efetuar a renovação durante o qual o aplicativo continua a funcionar. A disponibilidade e a duração do período de carência é definida pelo provedor de serviços.

Para usar o Kaspersky Security Center Cloud Console sob a assinatura, você precisa aplicar o código de ativação recebido do provedor de serviços.

Você pode aplicar um código de ativação diferente para o Kaspersky Security Center Cloud Console somente após sua assinatura expirar ou quando a cancelar.

Dependendo do provedor de serviços, o conjunto de ações possíveis para o gerenciamento da assinatura pode variar. O Provedor de Serviços não pode conceder nenhum período de carência para a renovação da assinatura, portanto o aplicativo perde sua funcionalidade.

Os códigos de ativação comprados sob a assinatura não podem ser usados para ativar versões anteriores do Kaspersky Security Center Cloud Console.

Ao usar o aplicativo sob a assinatura, o Kaspersky Security Center Cloud Console automaticamente tenta acessar o servidor de ativação em intervalos de tempo especificados até que a assinatura expire. Caso não seja possível acessar o servidor usando o DNS do sistema, o aplicativo usará os servidores DNS públicos. Você pode renovar sua assinatura no site do provedor de serviços.

Fornecimento de dados

O Kaspersky Security Center Cloud Console permite que o usuário identifique e controle dispositivos (e seus proprietários) conectados ao Kaspersky Security Center Cloud Console, por meio dos recursos dos aplicativos gerenciados.

Métodos de fornecimento de dados:

1. O usuário insere dados na interface do Kaspersky Security Center Cloud Console.
2. O Agente de Rede recebe dados do dispositivo e os transfere para o Servidor de Administração.
3. O Agente de Rede recebe extração de dados por o aplicativo gerenciado do Kaspersky e transfere para o Servidor de Administração. A lista de dados processados pelos aplicativos gerenciados da Kaspersky é fornecida na Ajuda desses aplicativos.
4. Os dados são transferidos de Servidores de Administração secundários em execução no local.

O Kaspersky Security Center Cloud Console exclui automaticamente os espaços de trabalho 30 dias após o término do período da licença de avaliação e 90 dias após o término do prazo da licença comercial.

Após a expiração do período da licença, a Kaspersky salva os dados do usuário relacionados a alertas e incidentes nos espaços de trabalho do usuário por 30 dias.

Sob a licença atual, o período de armazenamento para alertas e incidentes é de 360 dias. Após esse período, os alertas e incidentes mais antigos são excluídos automaticamente.

A exclusão final dos dados relacionados nesta seção pode levar até 24 horas.

Dados enviados para servidores Kaspersky

Dados enviados durante a ativação

Ao usar o Código de Ativação para ativar o Software, a fim de verificar a legitimidade do uso do software, o Usuário concorda em fornecer periodicamente à Kaspersky as seguintes informações:

- Código de ativação
- Identificador de ativação exclusivo para a licença atual

A Kaspersky também pode usar essas informações para gerar informações estatísticas sobre a distribuição e o uso do software da Kaspersky.

Dados enviados durante a atualização

Após o recebimento de atualizações dos servidores de atualização do titular dos direitos, a fim de melhorar a qualidade do mecanismo de atualização, o Usuário concorda em fornecer periodicamente as seguintes informações à Kaspersky:

- ID do software recebida da licença

- Versão completa do software
- ID de licença do software
- ID de instalação do software (PCID)
- ID de inicialização da atualização do software

A Kaspersky também pode usar essas informações para gerar informações estatísticas sobre a distribuição e o uso do software da Kaspersky.

Dados para garantir operação ininterrupta, trabalho eficiente e verificação do uso legítimo do Kaspersky Security Center Cloud Console

As seguintes informações podem ser usadas para a finalidade especificada:

- Nomes e versões dos aplicativos de segurança da Kaspersky conectados ao espaço de trabalho, bem como a quantidade de dispositivos nos quais eles aplicativos estão instalados.
- Número de dispositivos com aplicativos de segurança da Kaspersky instalados que tenham sido conectados a todos os espaços de trabalho, e a distribuição dos dispositivos conectados por tipo.
- Identificador do espaço de trabalho, identificador da empresa, país e região do espaço de trabalho e data de criação do espaço de trabalho.
- Número de usuários no espaço de trabalho, data da última autenticação no espaço de trabalho.
- Dados sobre a licença atualmente utilizada (tipo de licença, limite da licença para a quantidade de dispositivos, quantidade de dispositivos conectados e data de validade da licença usada anteriormente).

Dados transferidos ao seguir os links na interface do Kaspersky Security Center Cloud Console

Seguindo os links no Console de Administração ou Kaspersky Security Center Cloud Console, o usuário concorda com a transferência automática dos seguintes dados:

- Localização do Kaspersky Security Center Cloud Console
- ID da licença
- Se a licença foi adquirida por meio de um parceiro

A lista de dados fornecida via cada link depende da finalidade e da localização do link.

Dados necessários para o funcionamento do espaço de trabalho

O Kaspersky Security Center Cloud Console processa os seguintes dados:

1. Detalhes dos dispositivos detectados na rede da organização

   O Agente de Rede recebe os dados listados abaixo do dispositivo e os transfere para o Servidor de Administração:

a. Especificações técnicas do dispositivo detectado e seus componentes necessários para a identificação do dispositivo que foram recebidas por meio de sondagem de rede:

- Sondagem do Active Directory:

  Dispositivos Active Directory: nome distinto do dispositivo; nome de domínio do Windows recebido do controlador de domínio; nome do dispositivo no ambiente Windows; nome de domínio NetBIOS; domínio DNS e nome DNS do dispositivo; conta do Gerenciador de Contas de Segurança (SAM) (nome para fazer login no sistema usado para suporte de clientes e servidores que executam versões anteriores do sistema operacional, como Windows NT 4.0, Windows 95, Windows 98 e LAN Manager); nome distinto do domínio; nomes distintos dos grupos aos quais o dispositivo pertence; nome distinto do usuário que gerencia o dispositivo; e identificador global único (GUID) e GUID principal do dispositivo.

  Quando a rede do Active Directory é sondada, os seguintes tipos de dados também são processados, com o objetivo de exibir informações sobre a infraestrutura gerenciada e o uso dessas informações pelo usuário, por exemplo, durante a implementação da proteção:

- Unidades organizacionais do Active Directory: nome distinto da unidade organizacional; nome distinto do domínio; GUID e GUID primária da unidade organizacional.

- Domínios do Active Directory: nome de domínio do Windows recebido do controlador de domínio; domínio DNS; GUID do domínio.

- Usuários do Active Directory: nome de exibição do usuário; nome distinto do usuário; nome distinto do domínio; nome da organização do usuário; nome do departamento em que o usuário trabalha; nome distinto de outro usuário atuando como gerente do usuário; nome completo do usuário; conta SAM; endereço de e-mail; endereço de e-mail alternativo; número de telefone principal; número de telefone alternativo; número de celular; cargo do usuário; nomes distintos dos grupos aos quais o usuário pertence; identificador global único (GUID) do usuário; identificador de segurança do usuário (SID) (valor binário exclusivo usado para identificar o usuário como responsável de segurança); e nome principal do usuário (UPN) - nome de login no estilo da Internet para um usuário com base no padrão da Internet RFC 822. O UPN é mais curto que o nome distinto e mais fácil de lembrar. Por convenção, o UPN mapeia para o nome de e-mail do usuário.

- Grupos do Active Directory: nome distinto do grupo; endereço de email; nome distinto do domínio; conta SAM; nomes distintos de outros grupos aos quais o grupo pertence; SID do grupo; GUID do grupo.

b. Sondagem de domínio Samba:

Dispositivos Samba: nome distinto do dispositivo; nome de domínio recebido do controlador de domínio; nome do dispositivo NetBIOS; nome de domínio NetBIOS; domínio DNS e nome DNS do dispositivo; conta do Gerenciador de Contas de Segurança (SAM); nome distinto do domínio; nomes distintos dos grupos aos quais o dispositivo pertence; nome distinto do usuário que gerencia o dispositivo; Identificador Global Único (GUID) e o GUID principal do dispositivo.

- Unidades organizacionais do Samba: nome distinto da unidade organizacional; nome distinto do domínio; GUID e GUID principal da unidade organizacional.

- Domínios do Samba: nome de domínio recebido do controlador de domínio; domínio DNS; GUID do domínio.

- Usuários Samba: nome de exibição do usuário; nome distinto do usuário; nome da organização do usuário; nome do departamento onde o usuário trabalha; nome distinto de outro usuário atuando como gerente do usuário; nome completo do usuário; conta SAM; endereço de e-mail; endereço de e-mail alternativo; número de telefone principal; número de telefone alternativo; número de celular; nome do cargo do usuário; nomes distintos dos grupos aos quais o usuário pertence; Identificador Global Único (GUID) do usuário; Identificador de Segurança (SID) do usuário (valor binário exclusivo usado para identificar o usuário como uma entidade de segurança); nome principal do usuário (UPN) - nome de login no estilo da Internet para um usuário baseado no padrão da Internet RFC 822. O UPN é mais curto que o nome distinto e mais fácil de lembrar. Por convenção, o UPN mapeia para o nome de e-mail do usuário.

- Grupos do samba: nome distinto do grupo; endereço de e-mail; nome distinto do domínio; conta SAM; nomes distintos de outros grupos aos quais o grupo pertence; SID do grupo; GUID do grupo.

c. Sondagem de domínio Windows:

- Nome do domínio ou grupo de trabalho do Windows
- Nome do dispositivo NetBIOS
- Domínio DNS e nome DNS do dispositivo
- Nome e descrição do dispositivo
- Visibilidade do dispositivo na rede
- Endereço IP do dispositivo
- Tipo de dispositivo (estação de trabalho, servidor, SQL Server, controlador de domínio etc.)
- Tipo de sistema operacional instalado no dispositivo
- Versão do sistema operacional do dispositivo
- Horário da última atualização das informações sobre o dispositivo
- Horário em que o dispositivo foi visto pela última vez na rede

d. Sondagem de intervalo IP:

- Endereço IP do dispositivo
- Nome DNS ou nome NetBIOS do dispositivo
- Nome e descrição do dispositivo
- Endereço MAC do dispositivo
- Horário em que o dispositivo foi visto pela última vez na rede

2. Detalhes dos dispositivos gerenciados.

O Agente de Rede transfere os dados listados abaixo do dispositivo para o Servidor de Administração. O usuário digita o nome de exibição e a descrição do dispositivo na interface do Kaspersky Security Center Cloud Console:

a. Especificações técnicas do dispositivo gerenciado e seus componentes necessários para a identificação do dispositivo:

- Nome para exibição (gerado com base no nome NetBIOS, pode ser modificado manualmente) e descrição do dispositivo (inserido manualmente)
- Nome e tipo de domínio Windows (domínio Windows NT/grupo de trabalho do Windows)
- Nome do dispositivo no ambiente Windows
- Domínio DNS e nome DNS do dispositivo

- Endereço IP do dispositivo
- Máscara de sub-rede do dispositivo
- Localização da rede do dispositivo
- Endereço MAC do dispositivo
- Tipo de sistema operacional instalado no dispositivo
- Se o dispositivo é uma máquina virtual juntamente com o tipo de hipervisor
- Se o dispositivo é uma máquina virtual dinâmica como parte da VDI (Virtual Desktop Infrastructure)
- GUID do dispositivo
- ID da instância do Agente de Rede
- ID de instalação do Agente de Rede
- ID permanente do Agente de Rede

b. Outras especificações de dispositivos gerenciados e seus componentes necessários para a auditoria de dispositivos gerenciados e para tomar decisões sobre a aplicação de patches e atualizações específicas:

- Status do Windows Update Agent (WUA)
- Arquitetura do sistema operacional
- Fornecedor do sistema operacional
- Número do build do sistema operacional
- ID da versão do sistema operacional
- Pasta de localização do sistema operacional
- Se o dispositivo for uma máquina virtual - o tipo de máquina virtual
- Tempo de resposta do dispositivo
- Se o Agente de Rede está sendo executado no modo independente

c. Informações detalhadas sobre a atividade em dispositivos gerenciados:

- Data e hora da última atualização
- Data e hora em que o dispositivo foi visto pela última vez na rede
- Status de espera de reinicialização ("Reinicialização obrigatória.")
- Horário em que o dispositivo foi ligado

d. Detalhes das contas de usuário do dispositivo e as suas sessões de trabalho

e. Estatísticas de operação do ponto de distribuição se o dispositivo for um ponto de distribuição:

- Data e hora em que o ponto de distribuição foi criado
- Nome da pasta de trabalho
- Tamanho da pasta de trabalho
- Número de sincronizações com o Servidor de Administração
- Data e hora da última sincronização com o Servidor de Administração
- Número e tamanho total dos arquivos transferidos
- Número e tamanho total de arquivos baixados pelos clientes
- Volume de dados baixados pelos clientes usando o TCP (Protocolo de Controle de Transmissão)
- Volume de dados enviados aos clientes usando multicasting
- Volume de dados baixados por clientes usando multicasting
- Número de distribuições multicast
- Volume total de distribuição multicast
- Número de sincronizações com clientes após a última sincronização com o Servidor de Administração

f. Nome do Servidor de Administração virtual que gerencia o dispositivo

g. Detalhes dos dispositivos na nuvem:

- Região da nuvem
- Nuvem Privada Virtual (VPC)
- Zona de disponibilidade da nuvem
- Subrede da nuvem
- Grupo de posicionamento na nuvem

h. Detalhes de dispositivos móveis. O aplicativo gerenciado transfere esses dados do dispositivo móvel para o Servidor de Administração. A lista completa de dados está disponível na documentação do aplicativo gerenciado.

3. Detalhes dos aplicativos da Kaspersky instalados no dispositivo.

O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede:

a. Aplicativos Kaspersky gerenciados e componentes do Kaspersky Security Center Cloud Console instalados no dispositivo

b. Configurações dos aplicativos Kaspersky instalados no dispositivo gerenciado:

- Nome e versão do aplicativo Kaspersky
- Status

- Status da proteção em tempo real
- Data e hora da última verificação do dispositivo
- Número de ameaças detectadas
- Número de objetos não desinfetados
- Tarefas do aplicativo de segurança Kaspersky
- Disponibilidade e status dos componentes do aplicativo
- Hora da última atualização e versão dos bancos de dados antivírus
- Detalhes das configurações do aplicativo Kaspersky
- Informações sobre as chaves de licença ativas
- Informações sobre as chaves de licença reserva
- Data de instalação do aplicativo
- ID de instalação do aplicativo

c. Estatísticas de operação do aplicativo: eventos relacionados a alterações no status dos componentes do aplicativo Kaspersky no dispositivo gerenciado e desempenho de tarefas iniciadas pelos componentes do aplicativo

d. Status do dispositivo definido pelo aplicativo do Kaspersky

e. Marcações feitas por o aplicativo do Kaspersky

f. Conjunto de atualizações instaladas pare o aplicativo do Kaspersky:

- Nome de exibição, versão e idioma do aplicativo
- Nome interno do aplicativo
- Nome e versão do aplicativo da chave do registro
- Pasta de instalação do aplicativo
- Versão do patch
- Lista de patches instalados automaticamente pelos aplicativos
- Se o aplicativo compatível com o Kaspersky Security Center Cloud Console
- Se o aplicativo está instalado em um cluster

g. Detalhes dos erros de criptografia de dados nos dispositivos: ID do erro, hora da ocorrência, tipo de operação (criptografia/descriptografia), descrição do erro, caminho do arquivo, descrição da regra de criptografia, ID do dispositivo e nome do usuário

4. Eventos do Kaspersky Security Center Cloud Console e aplicativos gerenciados Kaspersky.

   O Agente de Rede transfere os dados do dispositivo para o Servidor de Administração.

A descrição de um evento pode conter os seguintes dados:

a. Nome do dispositivo

b. Nome do usuário do dispositivo

c. Nome do administrador que se conectou ao dispositivo remotamente

d. Nome, versão e fornecedor do aplicativo instalado no dispositivo

e. Caminho para a pasta de instalação do aplicativo no dispositivo

f. Caminho para o arquivo no dispositivo e nome do arquivo

g. Nome do aplicativo e parâmetros da linha de comando sob os quais o aplicativo foi executado

h. Nome do patch, nome do arquivo do patch, ID do patch, nível de vulnerabilidade corrigida pelo patch, descrição do erro de instalação do patch

i. Endereço IP do dispositivo

j. Endereço MAC do dispositivo

k. Status de reinicialização do dispositivo

l. Nome da tarefa que publicou o evento

m. Se o dispositivo mudou para o modo independente e o motivo da mudança

n. Informações sobre o problema de segurança no dispositivo: tipo de problema de segurança, nome do problema de segurança, nível de gravidade, descrição do problema de segurança, detalhes do problema de segurança transmitidos pelo aplicativo da Kaspersky

o. Tamanho do espaço livre em disco no dispositivo

p. Se o aplicativo Kaspersky está sendo executado no modo de funcionalidade limitada, IDs de escopos funcionais

q. Valor antigo e novo da configuração do aplicativo Kaspersky

r. Descrição do erro ocorrido quando o aplicativo Kaspersky ou qualquer um de seus componentes executou a operação

5. As configurações dos componentes do Kaspersky Security Center Cloud Console e aplicativos gerenciados Kaspersky estão disponíveis nas politicas e nos perfis das politicas.

   O usuário insere dados na interface do Kaspersky Security Center Cloud Console.

6. As configurações de tarefas dos componentes do Kaspersky Security Center Cloud Console e aplicativos gerenciados Kaspersky

   O usuário insere dados na interface do Kaspersky Security Center Cloud Console.

7. Dados processados pelo recurso de Gerenciamento de patches e vulnerabilidades.

   O Agente de Rede transfere os dados listados abaixo do dispositivo para o Servidor de Administração:

a. Detalhes sobre aplicativos e patches instalados nos dispositivos gerenciados (Registro de aplicativos). Aplicativos podem ser identificados nas informações sobre arquivos executados nos dispositivos por a função Controle de Aplicativos:

- ID do aplicativo/patch
- ID do aplicativo principal (para um patch)
- Nome e versão do aplicativo/patch
- Se o aplicativo/patch é um arquivo .msi do Windows Installer
- Fornecedor de aplicativos/patches
- ID do idioma de localização
- Data de instalação do aplicativo/patch
- Caminho de instalação do aplicativo
- Site de Suporte Técnico do fornecedor do aplicativo/patch
- Número de telefone do Suporte Técnico
- ID da instância do aplicativo instalado
- Comentário
- Chave de desinstalação
- Chave para instalação no modo silencioso
- Classificação de patches
- Endereço da web para informações adicionais sobre o patch
- Chave de registro do aplicativo
- Número do build do aplicativo
- SID do usuário
- Tipo de sistema operacional (Windows, Unix)

b. Informações sobre hardware detectado nos dispositivos gerenciados (Registro de hardware):

- ID do dispositivo
- Tipo de dispositivo (placa mãe, CPU, RAM, dispositivo de armazenamento em massa, adaptador de vídeo, placa de som, controlador de interface de rede, monitor, dispositivo de disco óptico)
- Nome do dispositivo
- Descrição
- Fornecedor

- Número de série
- Revisão
- Informações sobre o driver: desenvolvedor, versão, descrição e data de lançamento
- Informações sobre o BIOS: desenvolvedor, versão, número de série e data de lançamento
- Chipset
- Taxa de clock
- Número de núcleos da CPU
- Número de threads da CPU
- Plataforma da CPU
- Velocidade de rotação do dispositivo de armazenamento
- RAM: tipo, número da peça
- Memória de vídeo
- Codec da placa de som

c. Detalhes sobre vulnerabilidades em aplicativos de terceiros nos dispositivos gerenciados:

- Identificador de vulnerabilidades
- Nível de gravidade da vulnerabilidade (advertência, alto, crítico)
- Tipo de vulnerabilidade (Microsoft, terceiros)
- Endereço da página na qual a vulnerabilidade está descrita
- Horário de criação da entrada sobre a vulnerabilidade
- Nome do fornecedor
- Nome local do fornecedor
- ID do fornecedor
- Nome do aplicativo
- Nome local do aplicativo
- Código de instalação do aplicativo
- Versão do aplicativo
- Idioma de tradução do aplicativo
- Lista de tags CVE da descrição da vulnerabilidade

- Tecnologias de proteção da Kaspersky que bloqueiam a vulnerabilidade (Proteção contra Ameaças a Arquivos, Detecção de Comportamento, Proteção contra Ameaças da Web, Proteção contra Ameaças ao Correio, Prevenção de Intrusão de Host, Escudo ZETA)
- Caminho para o arquivo de objeto no qual a vulnerabilidade foi detectada
- Hora de detecção de vulnerabilidade
- IDs dos artigos da Base de Dados de Conhecimento sobre a descrição da vulnerabilidade
- IDs dos boletins de segurança da descrição da vulnerabilidade
- Lista de atualizações para a vulnerabilidade
- Se existe um exploit para a vulnerabilidade
- Se existe um malware para a vulnerabilidade

d. Detalhes sobre atualizações disponíveis para aplicativos de terceiros instalados em dispositivos gerenciados:

- Nome e versão do aplicativo
- Fornecedor
- Idioma de tradução do aplicativo
- Sistema operacional
- Lista de patches de acordo com a sequência de instalação
- Versão original do aplicativo no qual o patch foi aplicado
- Versão do aplicativo após a instalação do patch
- ID do patch
- Número da build
- Sinalizadores de instalação
- Contratos de Licença para o patch
- Se o patch é um prerrequisito para instalação de outros patches
- Lista de aplicativos instalados necessários e suas atualizações
- Fontes de informação sobre o patch
- Informações adicionais sobre o patch (endereços da web)
- Endereço da web para download do patch, nome do arquivo, versão, revisão e SHA-256

e. Detalhes sobre atualizações da Microsoft encontradas pelo recurso WSUS:

- Número de revisão da atualização

- Tipo de atualização da Microsoft (Driver, Software, Categoria, Detectoide)
- Atualize o nível de importância de acordo com o boletim do Microsoft Security Response Center (MSRC) (Baixo, Médio, Alto, Crítico)
- IDs dos boletins do MSRC relacionados à atualização
- IDs de artigos na Base de Conhecimento do MSRC
- Nome da atualização (cabeçalho)
- Descrição da atualização
- Se o instalador da atualização é interativo
- Sinalizadores de instalação
- Classificação da atualização (atualizações críticas, atualizações de definição, drivers, pacotes de recursos, atualizações de segurança, service packs, ferramentas, implementações de atualizações, atualizações e upgrade)
- Informações sobre o aplicativo ao qual a atualização se aplica
- ID do Contrato de Licença do Usuário Final (EULA)
- Texto do EULA
- Se o EULA deve ser aceito para ocorrer a instalação da atualização
- Informações sobre as atualizações associadas (ID e número de revisão)
- ID da atualização (identidade de atualização global do Microsoft Windows)
- IDs das atualizações substituídas
- Se a atualização está oculta
- Se a atualização é obrigatória
- Status de instalação da atualização (Não aplicável, Não designada para instalação, Designada, Instalando, Instalada, Com falha, Reinicialização obrigatória, Não designada para instalação (nova versão))
- IDs do CVE para a atualização
- Empresa que lançou a atualização ou o valor "Empresa ausente"

f. Lista de atualizações da Microsoft encontradas pelo recurso WSUS que devem ser instaladas no dispositivo.

8. Informações sobre os arquivos executáveis detectados nos dispositivos gerenciados pelo recurso Controle de Aplicativos (podem ser associadas à informação do Registro de aplicativos). Uma lista completa de dados é fornecida na seção que descreve os dados para dispositivos gerenciados pelo aplicativo correspondente.

   O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede.

9. Detalhes sobre arquivos colocados em Backup. Uma lista completa de dados é fornecida na seção que descreve os dados para dispositivos gerenciados pelo aplicativo correspondente.

   O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede.

10. Detalhes sobre arquivos solicitados pelos especialistas da Kaspersky para análise detalhada. Uma lista completa de dados é fornecida na seção que descreve os dados para dispositivos gerenciados pelo aplicativo correspondente.

    O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede.

11. Informações sobre status e acionamento das regras do Controle Adaptivo de Anomalias. Uma lista completa de dados é fornecida na seção que descreve os dados para dispositivos gerenciados pelo aplicativo correspondente.

    O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede.

12. Informações sobre dispositivos (unidades de memoria, ferramentas de transferência de informações, informação de ferramentas hardcopy e conexões de barramento) instalados ou conectados ao dispositivo gerenciado e detectados pelo recurso Controle de Dispositivos. Uma lista completa de dados é fornecida na seção que descreve os dados para dispositivos gerenciados pelo aplicativo correspondente.

    O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede.

13. Dados sobre alertas:

    - Data e hora do primeiro evento de telemetria no alerta
    - Data e hora do último evento de telemetria no alerta
    - Nome da regra acionada (o usuário o insere na interface do Kaspersky Security Center Cloud Console)
    - Status de alerta
    - Resolução (falso positivo, verdadeiro positivo, baixa prioridade)
    - ID e nome do usuário atribuído ao alerta
    - ID exclusiva no banco de dados do Kaspersky Security Center Cloud Console e nome do dispositivo relacionado aos eventos que são fontes de alerta
    - SID e nome do usuário do dispositivo relacionado aos eventos que são fontes de alerta
    - Observáveis, ou seja, dados observáveis relacionados aos eventos que são fontes de alerta:
        - Endereço IP
        - Soma de hash MD5 do arquivo e caminho do arquivo
        - Endereço da Web
        - Domínio
    - Detalhes adicionais do objeto relacionado ao alerta (recebido do aplicativo)

- Comentários para o alerta:
  - Data e hora em que o comentário foi adicionado
  - Usuário que adicionou o comentário
  - Texto do comentário
- Registro de alterações de alerta:
  - Data e hora da alteração
  - Usuário que realizou a alteração
  - Mudar descrição

14. Dados sobre problemas de segurança:
    - Data e hora do primeiro evento no problema de segurança
    - Data e hora do último evento no problema de segurança
    - Nome do problema de segurança (o usuário insere isso na interface do Kaspersky Security Center Cloud Console)
    - Breve descrição do problema de segurança
    - Prioridade do problema de segurança
    - Status do problema de segurança
    - ID e nome do usuário atribuído para o problema de segurança
    - Resolução (falso positivo, verdadeiro positivo, baixa prioridade, mesclado)
    - Comentário no problema de segurança:
      - Data e hora em que o comentário foi adicionado
      - Usuário que adicionou o comentário
      - Texto do comentário
    - Registro de alterações do problema de segurança:
      - Data e hora da alteração
      - Usuário que realizou a alteração
      - Mudar descrição
15. Dados processados pelo recurso de criptografia de dados dos aplicativos Kaspersky.

    O aplicativo gerenciado transfere os dados listados abaixo a partir do dispositivo para o Servidor de Administração por meio do Agente de Rede. O usuário digita a descrição da unidade na interface do Kaspersky Security Center Cloud Console:

a. Lista de unidades nos dispositivos:

- Nome da unidade
- Status de criptografia
- Tipo de unidade (inicialização ou disco)
- Número de série da unidade
- Descrição

b. Detalhes de erros de criptografia de dados nos dispositivos:

- Data e hora de quando o erro ocorreu
- Tipo de operação (criptografia, descriptografia)
- Descrição do erro
- Caminho do arquivo
- Descrição da regra
- ID do dispositivo
- Nome de usuário
- ID do Erro

c. As configurações de criptografia de dados do aplicativo Kaspersky.

Uma lista completa de dados é fornecida na seção que descreve os dados para dispositivos gerenciados pelo aplicativo correspondente.

16. Detalhes dos códigos de ativação inseridos.

O usuário insere dados na interface do Kaspersky Security Center Cloud Console.

17. Contas de usuários.

O usuário insere os dados listados abaixo na interface do Kaspersky Security Center Cloud Console:

a. Nome

b. Descrição

c. Nome completo

d. Endereço de e-mail

e. Número de telefone principal

f. Senha

18. Dados necessários para autenticação do usuário usando Active Directory:

a. Configurações dos Serviços de Federação do Active Directory (ADFS):

- URL principal do provedor de autenticação
- Certificados raiz confiáveis para ADFS
- ID do cliente gerada no ADFS
- Chave secreta para proteção de acesso ao ADFS
- Escopo dos tokens
- Domínio do Active Directory com o qual a integração é realizada
- Nome do campo de token contendo a SID do usuário
- Nome do campo de token contendo a matriz de SIDs dos grupos de usuários

O usuário insere dados na interface do Kaspersky Security Center Cloud Console.

b. Dados recebidos automaticamente do servidor ADFS pelo Kaspersky Security Center Cloud Console:

- Emissor (emissor)
- Endpoint de autorização do usuário (permission_endpoint)
- Endpoint de token (token_endpoint)
- URI do conjunto de chaves da web JSON (jwks_uri)
- Emissor de token de acesso (access_token_issuer)
- Endpoint de informações do usuário (userinfo_endpoint)
- Endpoint de sessão final (end_session_endpoint)
- Certificados de assinatura de token

19. Histórico de revisões de objetos de gerenciamento: Servidor de Administração, Grupo de administração, Política, Tarefa, Grupo de segurança do usuário, Pacote de instalação.

    O usuário insere os dados listados abaixo na interface do Kaspersky Security Center Cloud Console:

    a. Servidor de Administração

    b. Grupo de administração

    c. Política

    d. Tarefa

    e. Grupo Usuário/Segurança

    f. Pacote de instalação

20. Registro de objetos gerenciados excluídos.

    O usuário insere dados na interface do Kaspersky Security Center Cloud Console.

21. Pacotes de instalação criados dos arquivos e configurações de instalações.

    O usuário insere dados na interface do Kaspersky Security Center Cloud Console.

22. Dados necessários para a exibição de informativos da Kaspersky no Kaspersky Security Center Cloud Console:

    a. Informações sobre os aplicativos gerenciados Kaspersky usados pelo usuário: ID do aplicativo, número da versão completa.

    b. O usuário insere dados na interface do Kaspersky Security Center Cloud Console.

    c. Informações sobre a ativação do software no dispositivo: ID de licença do software; Prazo de licença de software; Data e hora de expiração da licença de software; tipo de licença de software usada; Tipo de assinatura de software; Data e hora de expiração da assinatura do software; Status atual da assinatura do Software; razão do status atual/variável da assinatura do Software; ID do item da lista de preços por meio do qual a licença do software foi adquirida.

    d. Informações sobre o acordo legal aceito pelo usuário durante o uso do software: tipo de acordo legal; versão do acordo legal; sinalizador de aceite dos termos do acordo legal pelo usuário.

    e. Informações sobre os anúncios recebidos do titular: ID do comunicado; hora de recebimento do comunicado; status de recebimento do comunicado.

    O usuário insere dados na interface do Kaspersky Security Center Cloud Console.

23. Configurações do usuário do Kaspersky Security Center Cloud Console.

    O usuário insere os dados listados abaixo na interface do Kaspersky Security Center Cloud Console:

    a. Idioma de tradução da interface do usuário

    b. Tema da interface do usuário

    c. Exibir configurações do painel de monitoramento

    d. Informações sobre o status das notificações: Já lida/Ainda não lida

    e. Status das colunas nas planilhas: Exibir/Ocultar

    f. Progresso do tutorial

24. Dados recebidos ao usar o recurso de diagnóstico remoto em um dispositivo gerenciado: arquivos de rastreamento, informações do sistema, detalhes dos aplicativos da Kaspersky instalados no dispositivo, arquivos de despejo, arquivos de log, resultados da execução de scripts de diagnóstico recebidos do Suporte Técnico.

25. Dados inseridos pelo usuário na interface do Kaspersky Security Center Cloud Console:

    a. Nome do grupo de administração ao criar uma hierarquia de grupos de administração

    b. Endereço de e-mail ao configurar notificações por e-mail

    c. Tags para dispositivos e regras de marcação

    d. Tags para aplicativos

    e. Categorias de usuários de aplicativos

f. Nome da função ao atribuir uma função a um usuário

g. Informações sobre sub-redes: nome, descrição, endereço e máscara da sub-rede

h. Configurações de relatórios e seleções

i. Quaisquer outros dados inseridos pelo usuário

26. Dados recebidos de um Servidor de Administração secundário implementado no local.

Os dados processados pelo servidor de administração do Kaspersky Security Center são descritos na ajuda on-line do Kaspersky Security Center.

Ao conectar um Servidor de Administração do Kaspersky Security Center implementado localmente como secundário em relação ao Kaspersky Security Center Cloud Console, o Kaspersky Security Center Cloud Console processa os seguintes tipos de dados do Servidor de Administração secundário:

a. Informações recebidas sobre os dispositivos na rede da organização como resultado da descoberta de dispositivos na rede do Active Directory ou na rede do Windows, ou por verificação de intervalos de IP

b. Informações sobre as unidades de organizações, domínios, usuários, e grupos do Active Directory recebidos como resultado de uma sondagem de rede do Active Directory

c. Informações sobre dispositivos gerenciados, suas especificações técnicas, incluindo aquelas necessárias para identificação do dispositivo, contas de usuários do dispositivo e suas sessões de trabalho

d. Informações dos dispositivos móveis transferidos usando o protocolo de Exchange ActiveSync

e. Informações dos dispositivos móveis transferidos usando o protocolo MDM do iOS

f. Detalhes dos aplicativos Kaspersky instalados no dispositivo: configurações, estatísticas de operação, status do dispositivo definido pelo aplicativo, atualizações instaladas e aplicáveis, tags

g. Dados contidos em eventos dos componentes do Kaspersky Security Center e aplicativos gerenciados Kaspersky

h. Configurações dos componentes do Kaspersky Security Center e Kaspersky gerenciados estão disponíveis nas politicas e nos perfis das politicas

i. Configurações de tarefas dos componentes do Kaspersky Security Center e aplicativos gerenciados Kaspersky

j. Dados processados pelo recurso Gerenciamento de patches e vulnerabilidades: detalhes de aplicativos e patches; informações sobre o hardware; detalhes de vulnerabilidades em software de terceiros detectados em dispositivos gerenciados; detalhes de atualizações disponíveis para aplicativos de terceiros; detalhes das atualizações da Microsoft encontradas pelo recurso WSUS

k. Categorias de usuários de aplicativos

l. Detalhes de arquivos executáveis detectados nos dispositivos gerenciados pelo recurso de Controle de Aplicativos

m. Detalhes sobre arquivos colocados em Backup

n. Detalhes sobre arquivos colocados em quarentene

o. Detalhes sobre arquivos requisitados por os especialistas da Kaspersky para análise detalhadas

p. Detalhes sobre status e ativação das regras do Controle Adaptivo de Anomalias

q. Detalhes sobre dispositivos (unidades de memoria, ferramentas de transferência de informações, informação de ferramentas hardcopy e conexões de barramentos) instalados ou conectados ao dispositivo gerenciado e detectado pelo recurso Controle de Aplicativos

r. Configurações de criptografia de aplicativos Kaspersky (repositório de chaves criptografia, status de criptografia do dispositivo)

s. Informações sobre os erros de criptografia de dados executados em dispositivos que usam o recurso Criptografia de dados dos aplicativos Kaspersky

t. Lista de controladores lógicos programáveis (PLCs) gerenciados

u. Detalhes dos códigos de ativação inseridos

v. Contas de usuário

w. Revisão de histórico de objetos gerenciados excluídos

x. Registro de objetos gerenciados excluídos

y. Pacotes de instalação criados dos arquivos e configurações de instalações

z. Configurações de usuário do Kaspersky Security Center Web Console

aa. Qualquer dado que o usuário inserir no Console de Administração ou na interface do Kaspersky Security Center Cloud Console

ab. Certificado de conexão segura de dispositivos gerenciados e componentes do Kaspersky Security Center

27. Informações carregadas do dispositivo gerenciado ao usar o recurso Diagnóstico Remoto: arquivos de diagnóstico (arquivos de dump, arquivos de log, arquivos de rastreamento etc.) e dados contidos nesses arquivos.

28. Dados necessários para a integração do Kaspersky Security Center Cloud Console a um sistema SIEM para exportação de eventos:

    - Dados necessários para conexão e autenticação:

        - Endereço e porta de conexão do sistema SIEM

        - Certificado de autenticação do servidor SIEM

        - Certificado confiável e chave privada para autenticação do cliente do Kaspersky Security Center Cloud Console no sistema SIEM

      O usuário insere dados na interface do Kaspersky Security Center Cloud Console.

    - Dados que recebidos do sistema SIEM pelo Kaspersky Security Center Cloud Console: chave pública do certificado do servidor SIEM para autenticação do servidor SIEM.

29. Dados necessários para a interação do Kaspersky Security Center Cloud Console com o ambiente em nuvem:

    a. Amazon Web Services (AWS):

- ID da chave de acesso da conta de usuário IAM
- Chave secreta da conta do usuário IAM

b. Microsoft Azure:

- ID do aplicativo Azure
- ID de assinatura do Azure
- Senha do aplicativo Azure
- Nome da conta para o repositório Azure
- Chave de acesso de conta para o repositório Azure

c. Google Cloud:

- E-mail do cliente Google
- ID do projeto
- Chave privada

O usuário insere dados na interface do Kaspersky Security Center Cloud Console.

30. Dados transferidos por um aplicativo Kaspersky não compatível

Ao instalar o Agente de Rede em um dispositivo que possui um aplicativo Kaspersky instalado, mas incompatível com o Kaspersky Security Center Cloud Console, esse aplicativo Kaspersky ainda transferirá dados para o Kaspersky Security Center Cloud Console. (A lista de dados é fornecida na seção "Sobre a coleta de dados" do sistema de Ajuda do aplicativo.) No entanto, o Kaspersky Security Center Cloud Console não poderá processar os dados transferidos pelo aplicativo incompatível da maneira como o processo é descrito para as principais funcionalidades do Kaspersky Security Center Cloud Console.

A lista de aplicativos Kaspersky compatíveis está disponível na Ajuda Online do Kaspersky Security Center Cloud Console.

Dados necessários para o funcionamento de aplicativos gerenciados

O seguinte aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração via Agente de Rede:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent
- Kaspersky Security for Windows Server
- Kaspersky Security for Mobile

- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux

A lista de dados processados é publicada em https://ksc.kaspersky.com/Home/LegalDocuments, no Acordo de Processamento de Dados do Kaspersky Security Center Cloud Console. Na página de documentos legais, localize o bloco de texto chamado Contrato do Kaspersky Security Center Cloud Console. Role a página para baixo até a seção Dados para dispositivos gerenciados via aplicativo gerenciado relevante. Você também pode usar a função Localizar padrão do seu navegador para isso.

Dados do usuário processados localmente

O único componente do Kaspersky Security Center que pode ser implementado localmente no Kaspersky Security Center Cloud Console é o Agente de rede.

Lista de dados do usuário processada localmente:

- Todos os dados listados na seção Dados do Usuário processados na estrutura e infraestrutura do Kaspersky, exceto os dados inseridos pelo administrador pela interface do Kaspersky Security Center Cloud Console
- Log de eventos do Agente de Rede Kaspersky
- Rastreamentos do Agente de Rede
- Logs, incluindo logs criados pelo instalador do Agente de Rede, pelos utilitários do Kaspersky Security Center

Os arquivos de dump, log e rastreamento do Agente de Rede contêm dados aleatórios e podem conter dados pessoais. Os arquivos são armazenados sem criptografia no dispositivo em que o Agente de rede está instalado. Os arquivos não são transferidos para o Kaspersky automaticamente. O usuário pode transferir esses dados para o Kaspersky manualmente, a pedido do Suporte Técnico, para solucionar problemas na operação do Kaspersky Security Center.

Processadores adicionais de dados pessoais

Além da Kaspersky, os processadores de dados pessoais relacionados ao espaço de trabalho do Kaspersky Security Center Cloud Console estão listados abaixo.

Nome e endereço da organização:
Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park, Leopardstown
Dublin 18 D18 P521

Serviço:
Microsoft Azure (hospedagem de dados)

Os países nos quais os dados são processados estão listados na seção "Seleção dos Data Centers usados para armazenar informações do Kaspersky Security Center Cloud Console".

Sobre documentos legais do Kaspersky Security Center Cloud Console

Para usar o Kaspersky Security Center Cloud Console, você deve ler e concordar com os termos e condições dos documentos legais especificados no site do Kaspersky Security Center Cloud Console. É possível visualizar os termos e condições da Política de Privacidade da AO Kaspersky Lab para sites ao fazer login no Kaspersky Security Center Cloud Console para gerenciar um espaço de trabalho. É possível ler o Contrato do Kaspersky Security Center Cloud Console e o Contrato de processamento de dados do Kaspersky Security Center Cloud Console ao criar um espaço de trabalho da empresa.

Leia atentamente os textos de todos os documentos legais antes de começar a usar o Kaspersky Security Center Cloud Console.

Contrato de Licença do Usuário Final para aplicativos Kaspersky

O Contrato de Licença do Usuário Final (doravante referido como Contrato de Licença ou EULA) é um contrato vinculativo entre você e a AO Kaspersky Lab que estipula os termos nos quais você pode usar o aplicativo.

É possível visualizar os termos do Contrato de Licença de Usuário Final usando os seguintes métodos:

- Na janela exibida durante a criação do pacote de instalação do aplicativo Kaspersky.
- No arquivo license.txt, na pasta de instalação do aplicativo Kaspersky, no dispositivo gerenciado.

Você pode revogar sua aceitação do Contrato de Licença do Usuário Final a qualquer momento.

Se você não aceitar os termos do Contrato de Licença para um aplicativo Kaspersky, não poderá usar o aplicativo.

Guia de Proteção

O Kaspersky Security Center Cloud Console é um aplicativo hospedado e mantido pela Kaspersky. Não é necessário instalar o Kaspersky Security Center Cloud Console em seu computador ou servidor. O Kaspersky Security Center Cloud Console permite que o administrador instale aplicativos de segurança da Kaspersky em dispositivos em uma rede corporativa, execute remotamente tarefas de verificação e atualização e gerencie as políticas de segurança dos aplicativos gerenciados.

O Kaspersky Security Center Cloud Console foi concebido para a execução centralizada de tarefas de administração e manutenção básicas na rede de uma organização. O aplicativo fornece ao administrador acesso a informações detalhadas sobre o nível de segurança da rede da organização. O Kaspersky Security Center Cloud Console permite configurar todos os componentes de proteção criados com o uso dos aplicativos Kaspersky.

O Kaspersky Security Center Cloud Console tem acesso total ao gerenciamento de proteção de dispositivos clientes, além de ser o componente mais importante do sistema de segurança da organização. Portanto, métodos de proteção maiores são necessários para o Kaspersky Security Center Cloud Console.

O Guia de Proteção descreve as recomendações e recursos de configuração do Kaspersky Security Center Cloud Console e seus componentes com o objetivo de reduzir os riscos de seu comprometimento.

O Guia de Proteção contém as seguintes informações:

- Configurar contas para acessar o Kaspersky Security Center Cloud Console
- Gerenciamento de proteção dos dispositivos cliente
- Configuração da proteção para aplicativos gerenciados
- Transferência de informações para aplicativos de terceiros

Antes de começar a trabalhar com o Kaspersky Security Center Cloud Console, haverá uma solicitação para que a versão resumida do guia de proteção seja lida.

Observe que não é possível usar o Kaspersky Security Center Cloud Console até confirmar que o Guia de Proteção foi lido.

Para ler o Guia de Proteção:

1. Abra o Kaspersky Security Center Cloud Console e faça login nele. O Kaspersky Security Center Cloud Console verifica se a leitura da versão atual do Guia de Proteção foi confirmada.

   Caso ainda não tenha lido o Guia de Proteção, uma janela será aberta e exibirá uma breve versão dele.

2. Execute uma das seguintes ações:

   - Caso queira visualizar a versão resumida do Guia de Proteção como um documento de texto, clique no link **Abrir em nova janela**.
   - Caso queira visualizar a versão completa do Guia de Proteção, clique no link **Abrir o Guia de Proteção na Ajuda Online**.

3. Depois de ler o Guia de Proteção, marque a caixa de seleção **Confirmo que li e compreendi totalmente o Guia de proteção** e, em seguida, clique no botão **Aceitar**.

Agora, é possível trabalhar com o Kaspersky Security Center Cloud Console.

Quando uma nova versão do Guia de Proteção aparecer, o Kaspersky Security Center Cloud Console solicitará a sua leitura.

Arquitetura do Kaspersky Security Center Cloud Console

Em geral, a escolha de uma arquitetura de gerenciamento centralizado depende da localização dos dispositivos protegidos, acesso a redes adjacentes, esquemas de entrega de atualizações do banco de dados e assim por diante.

Na fase inicial de desenvolvimento da arquitetura, recomendamos conhecer os componentes do Kaspersky Security Center Cloud Console e a interação entre eles, assim como os esquemas de tráfego de dados e uso de portas.

De acordo com essas informações, será possível formar uma arquitetura que especifique:

- Organização dos espaços de trabalho do administrador e métodos de conexão ao Kaspersky Security Center Cloud Console
- Os métodos de implementação do Agente de Rede e do software de proteção
- Usar pontos de distribuição
- Usar Servidores de Administração virtuais
- Usar uma hierarquia de Servidores de Administração
- O esquema de atualização do banco de dados de antivírus
- Outros fluxos de informação

Contas e autenticação

Usar a verificação em duas etapas com o Kaspersky Security Center Cloud Console

O **Kaspersky Security Center Cloud Console oferece o recurso de verificação em duas etapas** aos usuários.

A verificação em duas etapas pode ajudar a aumentar a segurança de sua conta no Kaspersky Security Center Cloud Console. Quando esse recurso é ativado, toda vez que entra no Kaspersky Security Center Cloud Console com o seu endereço de e-mail e senha, você insere um código de segurança adicional único. É possível receber um código de segurança único por SMS ou gerar esse código no aplicativo autenticador (dependendo do método de verificação em duas etapas configurado).

Recomendamos vivamente não instalar o aplicativo autenticador no mesmo dispositivo a partir do qual a conexão com o Kaspersky Security Center Cloud Console é estabelecida. É possível instalar um aplicativo autenticador no seu dispositivo móvel.

Proibição para salvar a senha do administrador

Quando o Kaspersky Security Center Cloud Console é usado, **recomendamos vivamente** não salvar a senha do administrador no navegador instalado no dispositivo do usuário.

Caso o navegador esteja comprometido, um intruso poderá obter acesso às senhas salvas. Além disso, caso um dispositivo de usuário com senhas salvas seja roubado ou perdido, um intruso poderá obter acesso aos dados protegidos.

Restrição da associação da função de administrador principal

Recomendamos restringir a participação na função de administrador principal.

Por padrão, depois que um usuário criar um espaço de trabalho, a função de administrador principal é atribuída a esse usuário. É útil para o gerenciamento, mas é crítico do ponto de vista da segurança, porque a função de administrador principal tem um extenso conjunto de privilégios. A atribuição dessa função aos usuários deve ser estritamente regulada.

É possível usar as funções de usuário predefinidas com um conjunto de direitos já configurados para a administração do Kaspersky Security Center Cloud Console.

Configuração de direitos de acesso aos recursos do aplicativo

Recomendamos usar a configuração flexível de direitos de acesso aos recursos do Kaspersky Security Center Cloud Console para cada usuário ou grupo de usuários.

O controle de acesso baseado em função permite a criação de funções de usuário padrão com um conjunto predefinido de direitos e atribuição dessas funções aos usuários dependendo de seu escopo de obrigações.

As principais vantagens do modelo de controle de acesso baseado em função:

- Facilidade de administração
- Hierarquia de função
- Abordagem de privilégio mínimo
- Segregação de deveres

É possível atribuir funções integradas a determinados profissionais de acordo com suas posições ou criar funções completamente novas.

Ao configurar as funções, observe os privilégios associados com a alteração do estado de proteção do dispositivo do Servidor de Administração e com a instalação remota de software de terceiros:

- Gerenciamento de grupos de administração.
- Operações com o Servidor de Administração.
- Instalação remota.
- Alteração dos parâmetros para armazenamento de eventos e envio de notificações.

  Esse privilégio permite definir as notificações que executam um script ou um módulo executável no dispositivo do Servidor de Administração quando um evento ocorrer.

Conta separada para instalação remota de aplicativos

Além da diferenciação básica de direitos de acesso, recomendamos restringir a instalação remota de aplicativos para todas as contas (exceto para o administrador principal ou outra conta especializada).

Recomendamos o uso de uma conta separada para instalação remota de aplicativos. É possível atribuir uma função ou permissões para a conta separada.

Gerenciamento de proteção dos dispositivos cliente

Regras automáticas para migrar os dispositivos entre os grupos de administração

Recomendamos restringir o uso de regras automáticas para dispositivos móveis entre os grupos de administração.

Se você usa as regras automáticas para mover dispositivos, isso poderá provocar a propagação de políticas que fornecem mais privilégios ao dispositivo do que ele tinha antes da realocação.

Além disso, mover um dispositivo cliente para outro grupo de administração pode causar a propagação das configurações da política. Essas configurações da política podem ser indesejáveis para distribuição entre os dispositivos convidados e não confiáveis.

Essa recomendação não se aplica à alocação inicial única de dispositivos para grupos de administração.

Requisitos de segurança para pontos de distribuição e gateways de conexão

Os dispositivos com o Agente de Rede instalado podem atuar como um ponto de distribuição e executar as seguintes funções:

- Distribuir atualizações e pacotes de instalação recebidos do Servidor de Administração para dispositivos clientes dentro do grupo.
- Executar a instalação remota de software de terceiros e aplicativos Kaspersky em dispositivos cliente.
- Faça a sondagem da rede para detectar novos dispositivos e para atualizar as informações sobre os existentes.
- Atua como um servidor proxy KSN para dispositivos cliente.

Tendo em vista as capacidades disponíveis, é recomendável proteger os dispositivos que funcionam como pontos de distribuição de qualquer tipo de acesso não autorizado (incluindo acesso físico).

Configuração da proteção para aplicativos gerenciados

Configuração da proteção da rede

Verifique e confirme se o cenário de configuração inicial do Kaspersky Security Center Cloud Console foi concluído. Esse cenário também inclui a execução das etapas do assistente de início rápido.

Quando o assistente de início rápido está em execução, as políticas e tarefas com parâmetros padrão são criadas. Esses parâmetros podem não ser os ideais ou até mesmo ser proibidos em sua organização. Portanto, recomendamos configurar as políticas e tarefas criadas e criar políticas e tarefas adicionais, se necessário, para a rede da organização.

Especificação da senha para desativar a proteção e desinstalar o aplicativo

Para evitar que invasores desativem os aplicativos de segurança Kaspersky, recomendamos vivamente ativar a proteção por senha para ativar a proteção e não permitir a desinstalação dos aplicativos de segurança Kaspersky. É possível definir a senha, por exemplo, para o Kaspersky Endpoint Security para Windows, Kaspersky Security for Windows Servers, Agente de rede e outros aplicativos Kaspersky. Depois de ativar a proteção por senha, recomendamos bloquear essas configurações com o fechamento do "cadeado".

Especificação da senha para a conexão manual de um dispositivo cliente ao Servidor de Administração (utilitário klmover)

O utilitário klmover permite conectar manualmente um dispositivo cliente ao Servidor de Administração. Ao instalar o Agente de Rede em um dispositivo cliente, o utilitário é copiado automaticamente para a pasta de instalação do Agente de Rede.

Para impedir que intrusos movam dispositivos para fora do controle do Servidor de Administração, é altamente recomendável ativar a proteção por senha para executar o utilitário klmover. Para ativar a proteção por senha, selecione a opção **Usar senha de desinstalação** nas configurações da política do Agente de Rede.

Ativar a opção **Usar senha de desinstalação** também ativa a proteção por senha para a Ferramenta de remoção do Kaspersky Security Center Web Console (cleaner.exe).

Usar a Kaspersky Security Network

Em todas as políticas de aplicativos gerenciados e nas propriedades do Kaspersky Security Center Cloud Console, é recomendável ativar o uso da Kaspersky Security Network (KSN) e aceitar a Declaração da KSN. Ao atualizar o Kaspersky Security Center Cloud Console, você pode aceitar a Declaração da KSN atualizada.

Descoberta de novos dispositivos

Recomendamos definir corretamente as configurações de descoberta de dispositivos: configure a integração com o Active Directory e especifique os intervalos de endereços IP para descobrir novos dispositivos.

De acordo com os propósitos de segurança, é possível usar o grupo de administração padrão que inclui todos os novos dispositivos e as políticas padrão que afetam esse grupo.

Transferência de eventos para sistemas de terceiros

Monitoramento e relatórios

Para uma resposta oportuna aos problemas de segurança, recomendamos configurar os recursos de monitoramento e relatórios.

Exportação de eventos para os sistemas SIEM

Para a detecção rápida dos problemas de segurança antes que ocorram danos significativos, recomendamos o uso da exportação de eventos em um sistema SIEM.

Notificações por e-mail de eventos de auditoria

Para uma resposta imediata a emergências, é recomendável configurar o Kaspersky Security Center Cloud Console para o envio de notificações sobre os eventos de auditoria, eventos críticos, eventos de falha e advertências que ele publica.

Como esses eventos são eventos intrassistema, pode haver um pequeno número deles, o que é bastante pertinente para a correspondência.

Configuração inicial do Kaspersky Security Center Cloud Console

Esta seção descreve o cenário principal de implementação do Kaspersky Security Center Cloud Console, começando pela criação do espaço de trabalho e terminando com o monitoramento do status da proteção de rede.

Para obter informações sobre a implementação do Kaspersky Security Center executado localmente, consulte a ajuda on-line do Kaspersky Security Center.

Recomendamos que você atribua no mínimo um dia útil para a conclusão do cenário.

O cenário orienta você pelas seguintes ações:

- Começando a trabalhar com um espaço de trabalho de sua empresa como administrador
- Detectar dispositivos em sua rede (se necessário, poderá atribuir pontos de distribuição e instalar manualmente pacotes de distribuição neles)
- Implementar aplicativos Kaspersky gerenciados nos dispositivos cliente; configurar ferramentas para proteção de rede, monitoramento e atualizações regulares dos bancos de dados, módulos de software e aplicativos Kaspersky

Ao concluir esse cenário, a proteção de rede baseada nos aplicativos Kaspersky será configurada. Você poderá prosseguir com o monitoramento do status de proteção da rede.

Pré-requisitos

Antes de começar:

- Visualize a arquitetura do Kaspersky Security Center Cloud Console para entender a interação entre os principais componentes do aplicativo.
- Leia as informações sobre o licenciamento do Kaspersky Security Center Cloud Console e aplicativos gerenciados.
- Verifique se você possui um código de ativação válido para o Kaspersky Security Center Cloud Console (se você estiver criando um espaço de trabalho comercial).

Fases

A configuração do Kaspersky Security Center Cloud Console em feita em fases:

1. **Configuração de portas**

   Certifique-se de que todas as portas necessárias estejam abertas para interação entre sua rede e a infraestrutura da Kaspersky. Além disso, caso planeje usar a hierarquia dos Servidores de Administração, certifique-se de que todas as portas necessárias estejam abertas para interação envolvendo o Servidor de Administração secundário (ou Servidores de Administração secundários) e os dispositivos clientes.

2. **Criar o espaço de trabalho para sua empresa**

   Crie uma conta, e então crie um espaço de trabalho para sua empresa.

3. **Executar o Assistente de início rápido**

Abra e faça login no Kaspersky Security Center Cloud Console. Ao fazer login pela primeira vez, automaticamente é solicitada a execução do Assistente de início rápido. Você também pode iniciar o Assistente de início rápido manualmente a qualquer momento.

Quando o Assistente de início rápido for concluído, você terá pacotes de instalação do Agente de Rede e aplicativos de segurança. Esses pacotes de instalação são necessários para a implementação adicional do Kaspersky Security Center Cloud Console.

4. **Implementação de aplicativos da Kaspersky**

   Execute o cenário de implementação inicial dos aplicativos da Kaspersky. Uma das etapas do cenário refere-se à operação de sondagem da rede. Esta operação é necessária para descobrir dispositivos clientes da sua rede. A sondagem da rede e suas configurações são descritas no cenário de descoberta de dispositivos em rede.

   Se você estiver implementando o Kaspersky Security for Windows Server, certifique-se de que os bancos de dados do aplicativo estejam atualizados.

5. **Licenciar aplicativos de segurança Kaspersky**

   Quando os aplicativos de segurança Kaspersky são implementados nos dispositivos gerenciados, eles devem ser licenciados aplicando um código de ativação à cada um dos aplicativos. Implemente seus códigos de ativação nos aplicativos Kaspersky instalados nos dispositivos gerenciados. Você tem várias opções para licenciar aplicativos de segurança da Kaspersky.

6. **Configuração da proteção da rede**

   Execute a configuração de proteção de rede para ajustar as políticas e tarefas criadas por meio do Assistente de início rápido.

7. **Atualização regular dos bancos de dados, módulos de software e aplicativos Kaspersky**

   Para manter sua rede protegida contra vírus e outras ameaças, você tem que configurar atualizações regulares dos bancos de dados, módulos de software e aplicativos da Kaspersky.

8. **Atualização de software de terceiros e correção de vulnerabilidades de software de terceiros (opcional)**

   O Kaspersky Security Center Cloud Console permite gerenciar as atualizações de aplicativos da Microsoft instalados em dispositivos cliente. Também é possível corrigir as vulnerabilidades em aplicativos da Microsoft por meio da instalação de atualizações necessárias.

9. **Configurar ferramentas para monitorar o status da proteção da rede**

   Selecione e configure widgets, relatórios e outras ferramentas que permitem monitorar o status da proteção da rede.

Quando o Kaspersky Security Center Cloud Console tiver sido implementado e configurado, você poderá prosseguir com o monitoramento do status da proteção da rede.

Gerenciamento do espaço de trabalho

Esta seção descreve como você pode usar contas e espaços de trabalho no Kaspersky Security Center Cloud Console.

Sobre o gerenciamento do espaço de trabalho no Kaspersky Security Center Cloud Console

Use o Kaspersky Security Center Cloud Console para fazer o seguinte:

- Criar uma conta.
- Editar uma conta.
- Registrar uma empresa e criar um espaço de trabalho.
- Editar informações sobre a empresa e os espaços de trabalho.
- Excluir um espaço de trabalho e uma empresa.
- Excluir uma conta.

Guia de Introdução ao Kaspersky Security Center Cloud Console

Esta seção descreve como se inscrever e começar a usar o Kaspersky Security Center Cloud Console.

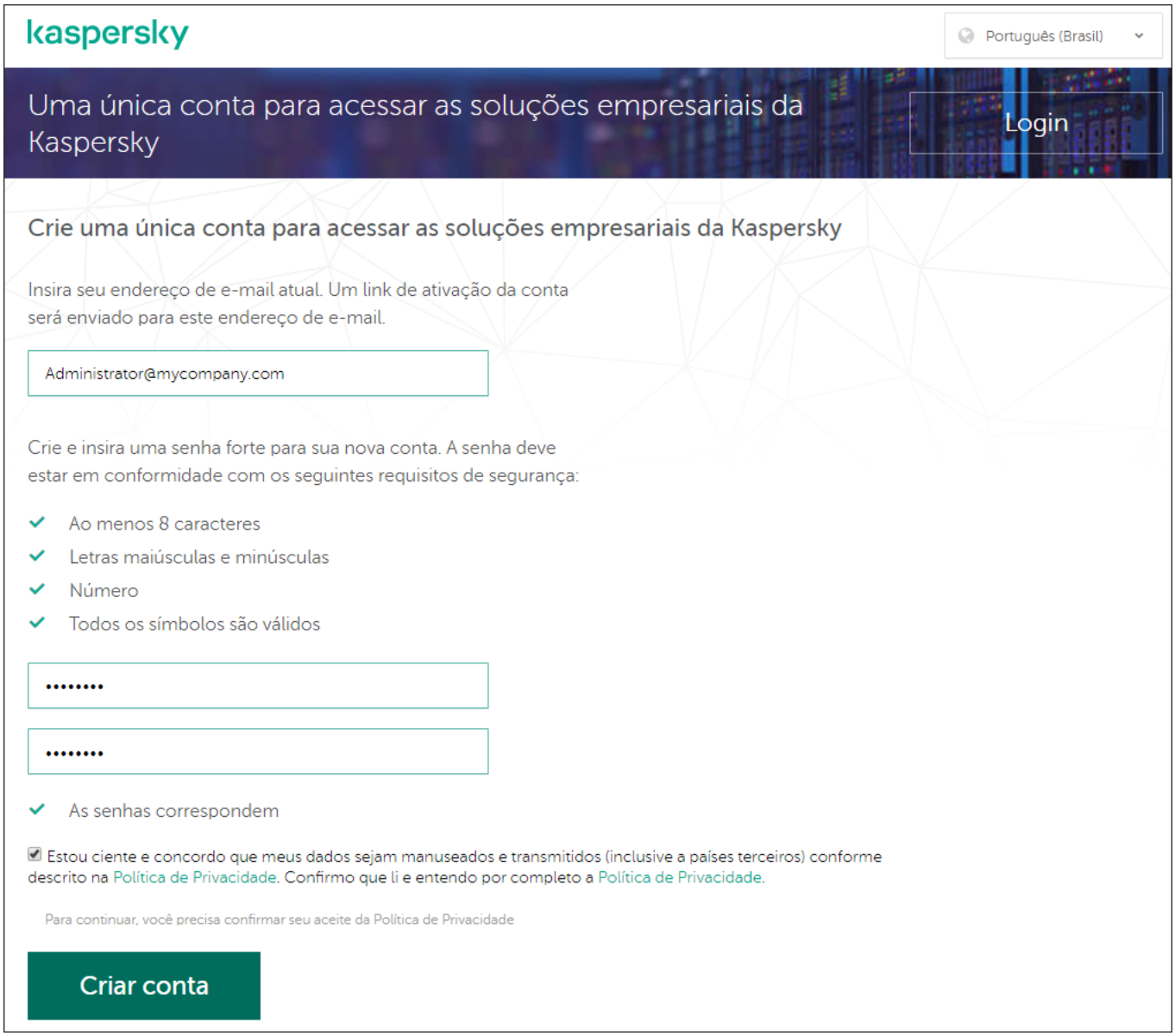
A inscrição no Kaspersky Security Center Cloud Console consiste nas seguintes etapas:

1. Criar e confirmar uma conta.
2. Registrar uma empresa e criar um espaço de trabalho.

Criar uma conta

Para criar uma conta no Kaspersky Security Center Cloud Console:

1. No navegador, acesse o Kaspersky Security Center Cloud Console.
2. Clique no botão **Criar uma conta** na página de início do Kaspersky Security Center Cloud Console.
3. Na página **Crie uma única conta para acessar as soluções empresariais da Kaspersky**, insira o endereço de e-mail, a senha e a confirmação de senha de sua conta (veja a figura abaixo).



Criar uma conta no Kaspersky Security Center Cloud Console

4. Clique no link **Política de Privacidade** e leia com atenção o texto da Política de Privacidade.

5. Se você está ciente e concorda que seus dados serão tratados e transmitidos (incluindo para países terceiros) conforme descrito na Política de Privacidade e confirma que leu e entendeu totalmente a Política de Privacidade, marque a caixa de seleção ao lado do texto de consentimento ao processamento de dados de acordo com a Política de Privacidade e clique no botão **Criar conta**.

   Caso não aceite a Política de Privacidade, não use o Kaspersky Security Center Cloud Console.

   O botão se torna disponível somente após você selecionara a caixa de seleção.

   Uma página solicitando que você verifique seu e-mail é exibida. Uma mensagem da Kaspersky é enviada para o endereço de e-mail que você especificou. A mensagem contém um link para concluir o procedimento de criação da conta.

6. Feche a página e abra a mensagem de e-mail na sua caixa de correio.

7. Clique no link na mensagem enviada pela Kaspersky para prosseguir para a página da sua conta.

8. Na página **Ativação da conta de usuário**, clique no botão **Continuar** para concluir a ativação da conta.

   A criação da conta no Kaspersky Security Center Cloud Console está concluída.

Registrar uma empresa e criar um espaço de trabalho

Logo após a criação da conta, você poderá registrar uma empresa e criar um espaço de trabalho para ela.

> Caso queira proteger mais de 10 mil dispositivos, não é preciso registrar uma empresa e criar um espaço de trabalho no Kaspersky Security Center Cloud Console como descrito abaixo. Em vez disso, envie uma solicitação ao Suporte Técnico da Kaspersky. Na solicitação, especifique as informações sobre a empresa e o espaço de trabalho que deseja criar.

Antes de iniciar, certifique-se de que saiba o seguinte:

- O nome da empresa na qual você pretende usar a solução de software.
- O país no qual em a empresa está localizada. Caso a empresa esteja localizada nos Estados Unidos ou Canadá, também é necessário saber o estado ou município.
- O número total de computadores e dispositivos móveis da empresa que deseja proteger.

Para registrar uma empresa e criar um espaço de trabalho no Kaspersky Security Center Cloud Console:

1. No navegador, acesse o Kaspersky Security Center Cloud Console.
2. Clique no botão **Login** na página de início do Kaspersky Security Center Cloud Console.
3. Insira o endereço de e-mail e a senha que você especificou ao criar a conta e clique no botão **Login**.

   O assistente para Criar um espaço de trabalho é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
4. Na página **Etapa 01: Termos de Uso do Kaspersky Security Center Cloud Console** do assistente, faça o seguinte:

   a. Leia cuidadosamente o Contrato, a Política de Privacidade e o Acordo de Processamento de Dados da solução de software.

   b. Se você concorda com os termos e condições do Contrato e do Contrato de Processamento de Dados e se estiver ciente e concorda que seus dados serão tratados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade, e você confirma que leu e entende por completo a Política de Privacidade, selecione as caixas de seleção ao lado dos três documentos listados e clique no botão **Aceitar**.

   > Se você não concordar com os termos e condições, não use o Kaspersky Security Center Cloud Console.

   > Ao clicar no botão **Declinar**, o processo de criação do espaço de trabalho não será concluído.
5. Na página **Etapa 02: Informações da empresa** do assistente, especifique os detalhes principais da empresa.

Preencha os campos a seguir:

- **Nome de sua empresa** (obrigatório)

  Especifique o nome da empresa na qual você pretende usar a solução de software. Você pode inserir uma sequência de caracteres com até 255 caracteres. A sequência de caracteres pode conter caracteres maiúsculos e minúsculos, numerais, espaços em branco, pontos, vírgulas, sinais de menos, traços e sublinhados. O nome da empresa especificado será exibido no Kaspersky Security Center Cloud Console.

- Campo **Descrição adicional da empresa** (opcional)

  Você pode especificar informações adicionais sobre a empresa registrada. Você pode inserir uma sequência de caracteres com até 255 caracteres. A sequência de caracteres pode conter caracteres maiúsculos e minúsculos, numerais, espaços em branco, pontos, vírgulas, sinais de menos, traços e sublinhados.

6. Na página **Etapa 03: Informações do espaço de trabalho** do assistente, especifique as informações sobre o espaço de trabalho que deseja criar para sua empresa.

   Preencha os seguintes campos obrigatórios:

   - **Nome do espaço de trabalho**. Especifique o nome do espaço de trabalho no qual você pretende usar a solução de software. Você pode inserir uma sequência de caracteres com até 255 caracteres. A sequência de caracteres pode conter caracteres maiúsculos e minúsculos, numerais, espaços em branco, pontos, vírgulas, sinais de menos, traços e sublinhados. O nome do espaço de trabalho especificado será exibido no Kaspersky Security Center Cloud Console.

   - **País**. Na lista suspensa, selecione o país em que seu espaço de trabalho está localizado. Se você selecionar Estados Unidos ou Canadá, especifique também o estado ou a província na lista suspensa **Estado**, exibida abaixo desse campo.

   - **Número de dispositivos**. Insira o número total de computadores e dispositivos móveis que você deseja proteger nesse espaço de trabalho.

     No campo de entrada, você pode inserir um número de 300 a 10.000.

7. Na página **Etapa 04: Licença para novo espaço de trabalho** do assistente, execute um dos seguintes procedimentos:

   - Se você quiser experimentar o Kaspersky Security Center Cloud Console, clique no link **Quero solicitar um espaço de trabalho de avaliação**.

     Recomendamos que você conecte seus próprios dispositivos ao seu espaço de trabalho de avaliação e teste quaisquer modificações nas configurações, observando os resultados.

     > Você não poderá alternar um espaço de trabalho de avaliação para o modo comercial inserindo um código de ativação. Para alternar para o modo comercial, você deve excluir o espaço de trabalho e criá-lo novamente.

   - Se quiser usar o Kaspersky Security Center Cloud Console no modo comercial, insira o código de ativação e clique no botão **Verificar**.

O registro de uma empresa e a criação de um espaço de trabalho no Kaspersky Security Center Cloud Console estão concluídos.

Após a preparação do espaço de trabalho, você receberá uma mensagem de e-mail com o link para acessá-lo.

Abrir seu espaço de trabalho do Kaspersky Security Center Cloud Console

Logo após a criação de um espaço de trabalho do Kaspersky Security Center Cloud Console, o espaço de trabalho é aberto automaticamente. Em seguida, é possível abrir o espaço de trabalho conforme descrito nesta seção.

Caso seja um administrador de um Servidor de Administração virtual, você terá acesso apenas ao Servidor de Administração virtual. Após o login e a abertura do espaço de trabalho, o Kaspersky Security Center Cloud Console fornece a interface do Servidor de Administração virtual. Não é possível mudar para o Servidor de Administração principal ou outros Servidores de Administração secundários.

Um administrador de um Servidor de Administração virtual deve ter acesso a um único Servidor de Administração virtual. Caso não tenha os direitos de acesso no servidor principal e os tenha em vários servidores virtuais, não será possível entrar no Kaspersky Security Center Cloud Console.

Para abrir seu espaço de trabalho do Kaspersky Security Center Cloud Console:

1. No navegador, acesse o Kaspersky Security Center Cloud Console.
2. Faça login na conta do Kaspersky Security Center Cloud Console, especificando o nome de usuário e a senha.
3. Caso tenha configurado a verificação em duas etapas, insira o código de segurança único enviado por SMS ou gerado no aplicativo autenticador (dependendo do método de verificação em duas etapas configurado).

   A página do portal exibe a empresa da qual você é administrador e a lista de seus espaços de trabalho.
4. Clique no nome do espaço de trabalho requerido ou no link **Ir para o espaço de trabalho** para prosseguir até o espaço de trabalho.

   Ocasionalmente, um espaço de trabalho pode estar indisponível devido a manutenções. Nesse caso, não será possível prosseguir para o espaço de trabalho do Kaspersky Security Center Cloud Console.

   Você não pode abrir um espaço de trabalho marcado para exclusão.
5. Se algum dos documentos legais do Kaspersky Security Center Cloud Console tiver sido alterado desde que você aceitou os termos e condições, a página do portal exibirá os documentos alterados.

   Faça o seguinte:

   a. Leia atentamente os documentos exibidos.

   b. Caso concorde com os termos e condições dos documentos exibidos, marque as caixas de seleção ao lado dos documentos listados e clique no botão **Eu aceito os termos**.

   Caso não concorde com os termos e condições, pare de usar a solução de software da Kaspersky selecionada.

   Se você clicar no botão **Eu não aceito**, a operação será encerrada.

Seu espaço de trabalho do Kaspersky Security Center Cloud Console é aberto.

Para sair do Kaspersky Security Center Cloud Console

Ao terminar seu trabalho, encerre com segurança sua sessão atual saindo do Kaspersky Security Center Cloud Console.

Para sair do Kaspersky Security Center Cloud Console,

No menu principal, acesse as configurações da conta e selecione **Sair**.

O Kaspersky Security Center Cloud Console é fechado e a página de acesso é exibida. Pode fechar esta página do navegador, se necessário. Todos os dados do seu espaço de trabalho serão salvos.

Gerenciar a empresa e a lista de espaços de trabalho

Esta seção descreve como visualizar as informações da empresa e a lista de espaços de trabalho registrados sob sua conta do Kaspersky Security Center Cloud Console, alterar informações sobre a empresa e os espaços de trabalho e excluir um espaço de trabalho ou empresa.

No momento, é possível registrar apenas uma empresa e criar um espaço de trabalho. Em versões futuras do Kaspersky Security Center Cloud Console, será possível criar espaços de trabalho adicionais para sua empresa. Isso ajudará a mapear a estrutura da empresa para os espaços de trabalho, criando um espaço de trabalho separado para cada filial.

Editar informações sobre uma empresa e um espaço de trabalho

É possível modificar as informações sobre uma empresa ou um espaço de trabalho especificado por você ao adicionar a empresa ao Kaspersky Security Center Cloud Console.

Para modificar informações sobre uma empresa e/ou um espaço de trabalho:

1. No navegador, acesse o Kaspersky Security Center Cloud Console.
2. Faça login na conta do Kaspersky Security Center Cloud Console, especificando o nome de usuário e a senha.
3. Caso tenha configurado a verificação em duas etapas, insira o código de segurança único enviado por SMS ou gerado no aplicativo autenticador (dependendo do método de verificação em duas etapas configurado).

   A página do portal exibe a empresa da qual você é administrador e uma lista dos seus espaços de trabalho.
4. Se quiser editar o nome e a descrição da empresa, faça o seguinte:
   a. Clique no ícone **Editar** (✎) na área com as informações da empresa.
   b. Modifique o nome e/ou a descrição da empresa como desejar.
   c. Clique no botão **Salvar**.

      Para cancelar as modificações, clique no botão **Cancelar**.
5. Se quiser editar o nome do espaço de trabalho, faça o seguinte:
   a. Clique no ícone **Editar** (✎) na área com as informações do espaço de trabalho.
   b. Modifique o nome do espaço de trabalho como desejar.

c. Clique no botão **Salvar**.

Para cancelar as modificações, clique no botão **Cancelar**.

As informações modificadas são exibidas no Kaspersky Security Center Cloud Console.

Excluir um espaço de trabalho e uma empresa

Um espaço de trabalho de uma empresa pode ser excluído manualmente ou automaticamente. Após a exclusão do último espaço de trabalho, as informações da empresa também serão excluídas automaticamente.

Exclusão manual

É possível excluir um espaço de trabalho de uma empresa se essa empresa tiver decidido deixar de usar o espaço de trabalho.

Após a exclusão de um espaço de trabalho, todos os aplicativos de segurança permanecerão nos dispositivos gerenciados. Portanto, recomendamos que antes de excluir o espaço de trabalho, você desative a proteção por senha de todos os aplicativos de segurança ou desinstale os aplicativos de segurança dos dispositivos gerenciados.

Para excluir um espaço de trabalho e uma empresa:

1. No navegador, acesse o Kaspersky Security Center Cloud Console.
2. Faça login na conta do Kaspersky Security Center Cloud Console, especificando o nome de usuário e a senha.
3. Caso tenha configurado a verificação em duas etapas, insira o código de segurança único enviado por SMS ou gerado no aplicativo autenticador (dependendo do método de verificação em duas etapas configurado).

   A página do portal exibe a empresa da qual você é administrador e uma lista dos seus espaços de trabalho.
4. Selecione o espaço de trabalho que deseja excluir.
5. À direita, na seção que contém o espaço de trabalho selecionado, clique no ícone **Excluir** (🗑).

   A janela **Excluir espaço de trabalho** é aberta.
6. Na janela **Excluir espaço de trabalho**, confirme que você deseja excluir o espaço de trabalho.

O espaço de trabalho é marcado para exclusão. O bloco de informações do espaço de trabalho é realçado com uma borda vermelha.

O bloco de informações do espaço de trabalho é duplicado na parte inferior da página, na seção **Marcados para exclusão**.

Você não pode acessar um espaço de trabalho que está marcado para a exclusão e gerenciá-lo.

Caso não consiga marcar um espaço de trabalho para exclusão, entre em contato com o Suporte Técnico da Kaspersky. Depois que um engenheiro do Suporte Técnico da Kaspersky receber a sua solicitação, o espaço de trabalho e a empresa serão removidos.

Os espaços de trabalho marcados para excluir podem permanecer nesse status durante um período de sete dias após terem sido marcados. Após sete dias, eles são excluídos automaticamente.

Durante esse período, você pode forçar a exclusão de um espaço de um espaço de trabalho marcado para a exclusão ou cancelar a exclusão de um espaço de trabalho.

Para forçar a exclusão de um espaço de trabalho:

1. No navegador, acesse o Kaspersky Security Center Cloud Console.
2. Faça login na conta do Kaspersky Security Center Cloud Console, especificando o nome de usuário e a senha.
3. Caso tenha configurado a verificação em duas etapas, insira o código de segurança único enviado por SMS ou gerado no aplicativo autenticador (dependendo do método de verificação em duas etapas configurado).

   A página do portal exibe a empresa da qual você é administrador e uma lista dos seus espaços de trabalho.
4. Na seção **Marcados para exclusão**, no bloco de informações do espaço de trabalho marcado para a exclusão, clique na opção **Forçar a remoção**.

   A janela **Excluir espaço de trabalho** é aberta.
5. Na janela **Excluir espaço de trabalho**, insira o ID do espaço de trabalho que deseja excluir.

   Será solicitado que você confirme o ID do espaço de trabalho para garantir que você não está excluindo o espaço de trabalho errado. Após um espaço de trabalho ter sido removido, ele não poderá ser restaurado.

   A ID do espaço de trabalho é exibida na seção de informações do espaço de trabalho abaixo do seu nome.
6. Na janela **Excluir espaço de trabalho**, clique em **OK**.

O espaço de trabalho é excluído. Todos os dados sobre usuários, dispositivos gerenciados e suas respectivas configurações são excluídos.

Exclusão automática

O Kaspersky Security Center Cloud Console exclui automaticamente um espaço de trabalho:

- 30 dias após a licença de avaliação expirar.
- 90 dias após todas as licenças comerciais ou de assinatura no repositório do Servidor de Administração expirarem.
- 90 dias após a exclusão da última chave de licença (ativa, reserva ou não em uso) adicionada manualmente no repositório.

O Kaspersky Security Center Cloud Console notifica os administradores do espaço de trabalho 30 dias, 7 dias e 1 dia antes de exclusão.

Cancelar exclusão de um espaço de trabalho

Você pode cancelar a remoção de um espaço de trabalho que foi marcado para exclusão.

Você não pode cancelar a remoção de um espaço de trabalho que já foi excluído.

Para cancelar a remoção de um espaço de trabalho:

1. No navegador, acesse o Kaspersky Security Center Cloud Console.
2. Faça login na conta do Kaspersky Security Center Cloud Console, especificando o nome de usuário e a senha.
3. Caso tenha configurado a verificação em duas etapas, insira o código de segurança único enviado por SMS ou gerado no aplicativo autenticador (dependendo do método de verificação em duas etapas configurado).

   A página do portal exibe a empresa da qual você é administrador e uma lista dos seus espaços de trabalho.
4. Na seção **Marcados para exclusão**, no bloco de informações do espaço de trabalho marcado para a exclusão, clique no link **Cancelar a remoção**.

A exclusão do espaço de trabalho é cancelada. Agora, você pode acessar o espaço de trabalho e continuar trabalhando com ele.

Gerenciar o acesso à empresa e aos espaços de trabalho

Esta seção contém informações sobre como conceder e revogar o acesso à empresa e seus espaços de trabalho.

O Kaspersky Security Center Cloud Console oferece dois níveis de acesso:

- **Administrador**

  Um usuário com este nível de acesso pode gerenciar totalmente a empresa e seus espaços de trabalho.
- **Usuário**

  Um usuário com este nível de acesso pode visualizar a lista de espaços de trabalho disponíveis e entrar nelas.

Conceder o acesso à empresa e aos espaços de trabalho

Você pode conceder acesso à sua empresa e aos espaços de trabalho se quiser que outro usuário possa fazer login na empresa e gerenciá-la de acordo com o nível de acesso selecionado.

Antes de conceder acesso a um usuário, o usuário deve criar uma conta no Kaspersky Security Center Cloud Console.

Para conceder acesso à empresa e seus espaços de trabalho:

1. No navegador, acesse o Kaspersky Security Center Cloud Console.
2. Faça login na conta do Kaspersky Security Center Cloud Console, especificando o nome de usuário e a senha.
3. Caso tenha configurado a verificação em duas etapas, insira o código de segurança único enviado por SMS ou gerado no aplicativo autenticador (dependendo do método de verificação em duas etapas configurado).

A página do portal exibe a empresa da qual você é administrador e uma lista dos seus espaços de trabalho.

4. Clique no link **Mostrar controle de acesso**.

   A lista de contas com acesso à empresa se expande.

5. Clique no link **Conceder acesso**.

6. No campo **Endereço de e-mail**, especifique o endereço de e-mail da conta à qual deseja conceder acesso.

7. Na lista **Nível de acesso**, selecione o nível de acesso que deseja atribuir à conta inserida:

   - **Administrador**

     Um usuário com este nível de acesso pode gerenciar totalmente a empresa e seus espaços de trabalho.

   - **Usuário**

     Um usuário com este nível de acesso pode visualizar a lista de espaços de trabalho disponíveis e entrar nelas.

   Não é possível conceder vários níveis de acesso à mesma conta na mesma empresa.

8. Clique no botão **Conceder**.

A conta especificada recebe acesso à empresa e seus espaços de trabalho. O usuário pode fazer login na empresa e gerenciá-la de acordo com o nível de acesso selecionado.

Se você concedeu o nível de acesso de **Usuário** à conta, deverá atribuir uma função ao usuário adicionado. Caso contrário, o usuário não poderá entrar no espaço de trabalho.

Revogar o acesso à empresa e aos espaços de trabalho

Você pode revogar o acesso à sua empresa e seus espaços de trabalho se não quiser mais que um usuário possa efetuar login na empresa e gerenciá-la (por exemplo, depois que o usuário sair da empresa).

Você não pode revogar seu próprio acesso à empresa.

Para revogar o acesso à empresa e seus espaços de trabalho:

1. No navegador, acesse o Kaspersky Security Center Cloud Console.

2. Faça login na conta do Kaspersky Security Center Cloud Console, especificando o nome de usuário e a senha.

3. Caso tenha configurado a verificação em duas etapas, insira o código de segurança único enviado por SMS ou gerado no aplicativo autenticador (dependendo do método de verificação em duas etapas configurado).

   A página do portal exibe a empresa da qual você é administrador e uma lista dos seus espaços de trabalho.

4. Clique no link **Mostrar controle de acesso**.

   A lista de contas com acesso à empresa se expande.

5. Clique no ícone **Revogar** (🗑) ao lado da conta cujo acesso você deseja revogar.

6. Na janela **Revogar acesso à empresa** que é aberta, clique em **OK** para confirmar a operação.

O acesso da conta selecionada à empresa e seus espaços de trabalho foi revogado. O usuário não pode mais fazer login na empresa e gerenciá-la.

Redefinir a senha

Caso esqueça a senha de sua conta do Kaspersky Security Center Cloud Console, é possível restaurar o acesso à conta redefinindo sua senha.

Para redefinir a senha de sua conta:

1. No navegador, acesse o Kaspersky Security Center Cloud Console.

2. Clique no botão **Login** e, em seguida, clique no link **Esqueceu a senha?**.

3. Digite o endereço de e-mail que especificou ao criar sua conta.

4. Clique em **Redefinir senha**.

   Uma mensagem de e-mail contendo um link para redefinir a senha é enviada para o endereço especificado.

5. Clique no link da mensagem de e-mail.

6. Na janela que se abre, digite uma nova senha e confirme-a.

7. Caso tenha configurado uma pergunta secreta, responda a essa pergunta.

   Caso tenha configurado a verificação em duas etapas, insira o código de segurança único enviado por SMS ou gerado no aplicativo autenticador (dependendo do método de verificação em duas etapas configurado).

8. Clique em **Continuar**.

   A nova senha para acessar o Kaspersky Security Center Cloud Console é salva.

Caso não tenha recebido uma mensagem de e-mail, verifique o endereço digitado, a pasta de spam e, em seguida, tente novamente. Caso não receba uma mensagem ao tentar novamente, o endereço de e-mail especificado provavelmente não está registrado no site. Entre em contato com o Suporte Técnico da Kaspersky.

Editar as configurações de uma conta no Kaspersky Security Center Cloud Console

Esta seção fornece instruções sobre como editar e excluir uma conta no Kaspersky Security Center Cloud Console.

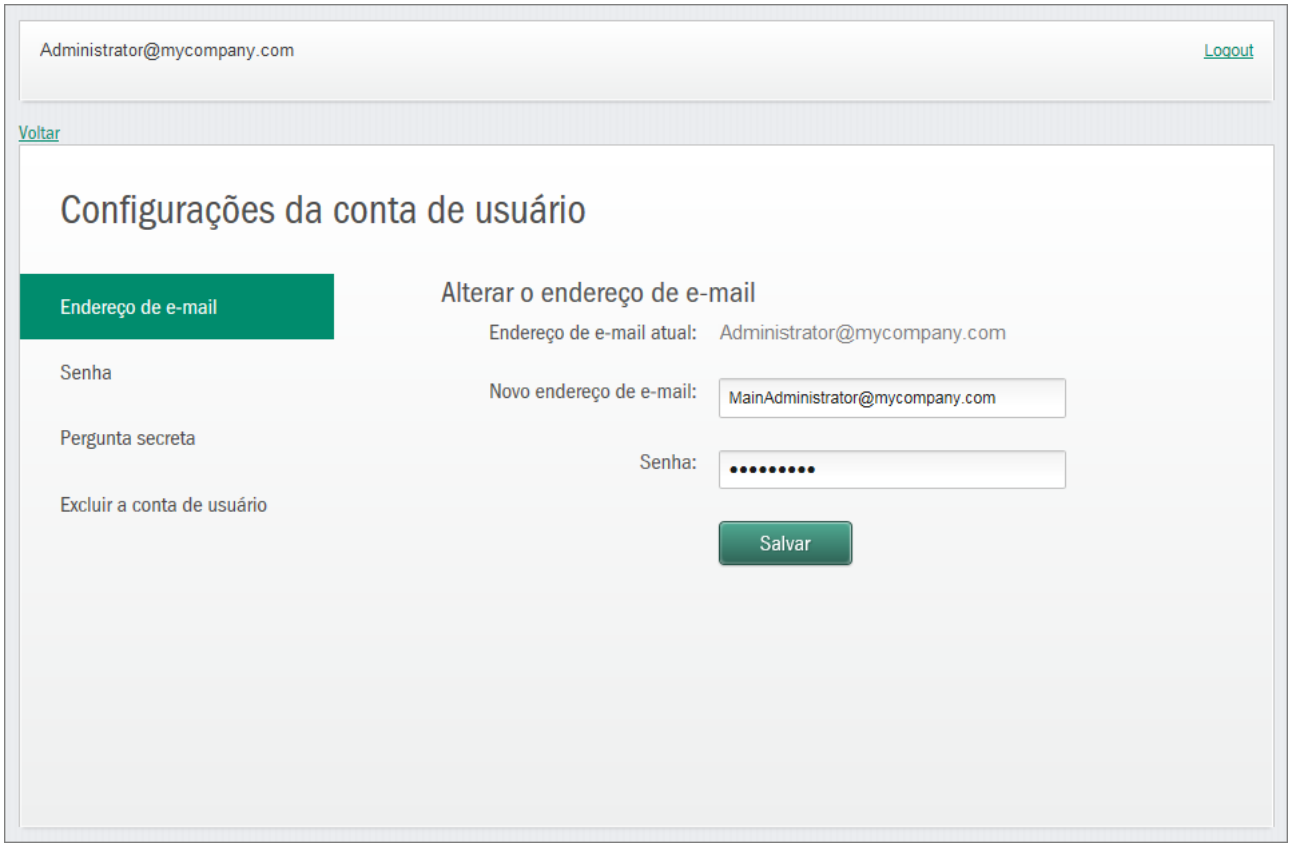
Alterar o endereço de e-mail

Para alterar o endereço de e-mail nas configurações da sua conta no Kaspersky Security Center Cloud Console:

1. No Kaspersky Security Center Cloud Console, clique no link com o nome da conta e selecione **Gerenciar a conta de usuário**.

   A janela **Configurações da conta de usuário** é aberta.

2. Selecione a seção **Endereço de e-mail** (veja a figura abaixo).



Alterar o endereço de e-mail nas configurações da conta no Kaspersky Security Center Cloud Console

   A seção **Endereço de e-mail** exibe o seu endereço de e-mail atual, um campo de entrada para inserir o novo endereço, um campo de entrada para inserir a senha e o botão **Salvar**.

3. No campo de entrada **Novo endereço de e-mail**, insira o seu novo e-mail.

   Insira o endereço cuidadosamente. Se você inserir um endereço inválido, não poderá prosseguir para a conta e usar o Kaspersky Security Center Cloud Console.

4. No campo de entrada **Senha**, digite sua senha atual.

5. Clique no botão **Salvar**.

6. Volte ao Kaspersky Security Center Cloud Console clicando no link **Voltar** ou saia do portal clicando no link **Logout**.

Seu endereço de e-mail foi alterado nas configurações das contas do Kaspersky Security Center Cloud Console e do My Kaspersky. Uma mensagem é enviada ao seu novo endereço de e-mail para notificá-lo de que o endereço de acesso à conta foi alterado. Na próxima vez que você fizer o login no Kaspersky Security Center Cloud Console, será necessário especificar seu novo endereço de e-mail.

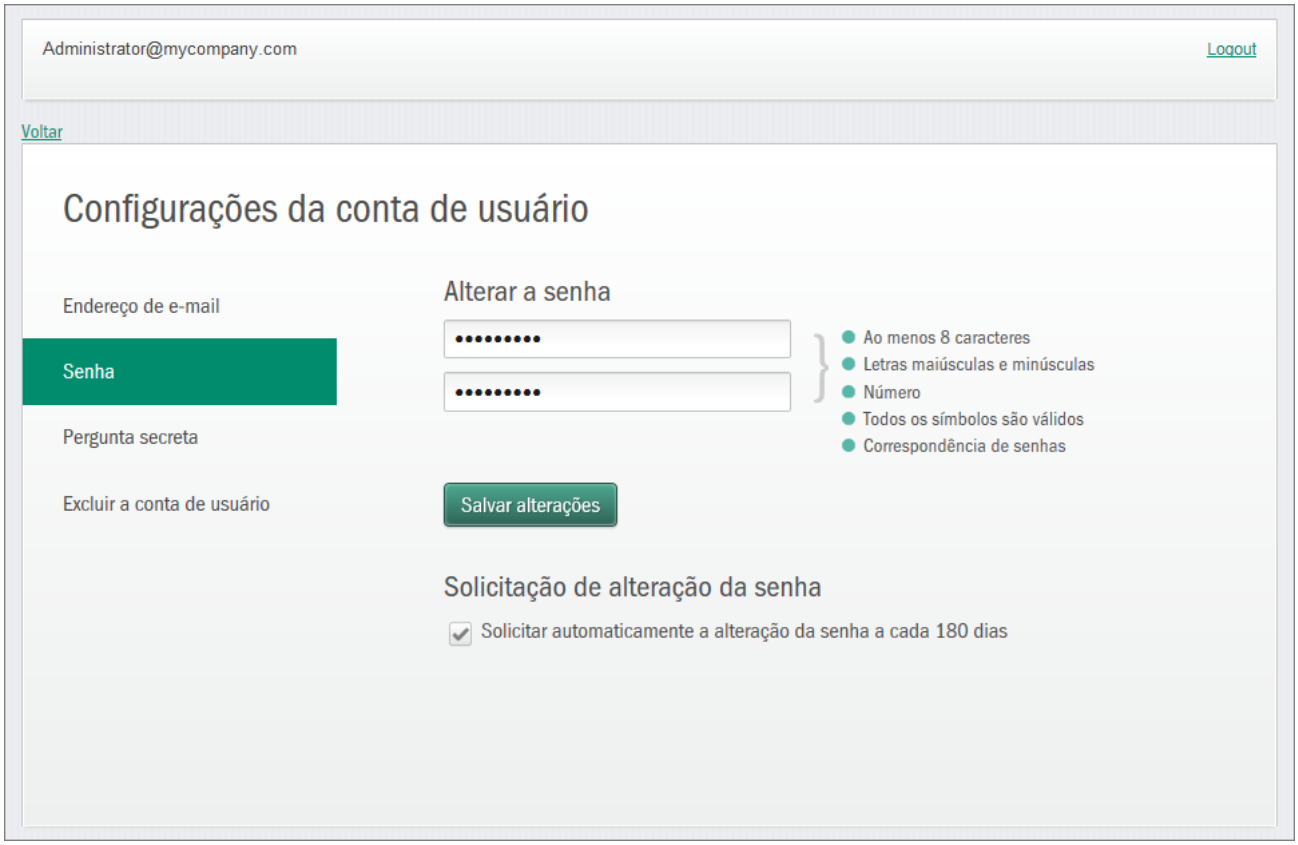
Alterar uma senha

Para alterar a senha nas configurações da conta no Kaspersky Security Center Cloud Console:

1. No Kaspersky Security Center Cloud Console, clique no link com o nome da conta e selecione **Gerenciar a conta de usuário**.

   A janela **Configurações da conta de usuário** é aberta.

2. Selecione a seção **Senha** (veja a figura abaixo).



Alterar a senha da conta no Kaspersky Security Center Cloud Console

   Esta seção exibe campos de entrada para inserir uma nova senha e confirmá-la, bem como o botão **Salvar alterações**.

3. Insira uma nova senha e confirme-a nos respetivos campos de entrada.

   À direita do campo de entrada de senha, os requisitos para a senha são mostrados. Você não pode salvar a nova senha até que você cumpra com os requisitos.

4. Marque ou desmarque a caixa de seleção **Solicitar automaticamente a alteração da senha a cada 180 dias**.

   Por padrão, esta caixa de seleção está selecionada.

5. Clique no botão **Salvar alterações**.

6. Volte ao Kaspersky Security Center Cloud Console clicando no link **Voltar** ou saia do portal clicando no link **Logout**.

Sua senha foi alterada. Você terá de inserir a nova senha ao fazer o login no Kaspersky Security Center Cloud Console e no portal My Kaspersky.

Usar a verificação em duas etapas

Esta seção descreve a verificação em duas etapas, cujo objetivo é aumentar a segurança de sua conta no Kaspersky Security Center Cloud Console.

Sobre a verificação em duas etapas

A verificação em duas etapas pode ajudar a aumentar a segurança de sua conta no Kaspersky Security Center Cloud Console. Quando esse recurso é ativado, toda vez que entra no Kaspersky Security Center Cloud Console com o seu endereço de e-mail e senha, você insere um código de segurança adicional único. Com a verificação em duas etapas, os criminosos não podem entrar em sua conta se roubarem ou adivinharem sua senha, eles devem também ter acesso ao seu telefone celular. Além disso, quando a verificação em duas etapas estiver ativada, você deve digitar um código de segurança adicional único se esquecer a senha.

Após configurar a verificação em duas etapas, você não é apenas responsável por manter o celular fisicamente protegido, mas também pela manutenção do acesso ao seu número de telefone.

É possível receber um código de segurança único por uma das seguintes maneiras:

- Um código de segurança é enviado via SMS para o seu número de celular.

  Nesse caso, se você perder o acesso ao seu telefone celular, não poderá fazer login na conta do Kaspersky Security Center Cloud Console até restaurar o acesso ao seu número de telefone.

- Um código de segurança é gerado em um aplicativo autenticador instalado no seu celular.

  Recomendamos veementemente configurar a verificação em duas etapas por meio de um aplicativo autenticador. Nesse caso, é possível fazer login na conta mesmo que seu telefone celular não esteja conectado à Internet ou uma rede móvel.

  Nós testamos apenas o Google Authenticator e o Microsoft Authenticator para verificar a compatibilidade com o Kaspersky Security Center Cloud Console, e esses aplicativos eram gratuitos na época. As interfaces dos aplicativos podem não estar disponíveis no idioma de preferência. Verifique também a conformidade com a GDPR e as políticas de privacidade antes de usar os aplicativos. A Kaspersky não é de forma alguma patrocinada, apoiada ou afiliada a qualquer um dos proprietários desses aplicativos.

  > O Microsoft Authenticator pode ser instalado apenas em dispositivos móveis.

  Também recomendamos instalar um aplicativo autenticador em um dispositivo que não seja o celular. Dessa forma, será possível entrar em sua conta se o celular for perdido ou roubado.

  Nesse caso, se você perder o acesso ao seu telefone celular e não tiver um aplicativo autenticador em outro dispositivo, não poderá fazer login na conta do Kaspersky Security Center Cloud Console até restaurar o acesso ao seu número de telefone. Depois disso, use o código de segurança enviado por SMS.

> Caso tenha configurado anteriormente uma pergunta secreta para restaurar a senha se ela for perdida, o recurso de pergunta de segurança será desativado permanentemente após a configuração da verificação em duas etapas.

Cenário: Configuração da verificação em duas etapas

A verificação em duas etapas pode ajudar a aumentar a segurança de sua conta no Kaspersky Security Center Cloud Console. Após completar o cenário nesta seção, a verificação de sua conta em duas etapas será configurada.

O cenário continua em estágios:

1. **Adicione o seu número de telefone**

   Nesta etapa, o usuário configura a verificação em duas etapas via SMS.

2. **Instalação e configuração do aplicativo autenticador**

   Instale e configure o aplicativo autenticador.

   Recomendamos veementemente configurar a verificação em duas etapas por meio de um aplicativo autenticador. Nesse caso, é possível fazer login na conta mesmo que seu telefone celular não esteja conectado à Internet ou uma rede móvel.

   Também recomendamos instalar um aplicativo autenticador em um dispositivo que não seja o celular. Dessa forma, será possível entrar em sua conta se o celular for perdido ou roubado.

3. **Altere o seu número de telefone**

   Caso necessário, é possível alterar o número de telefone utilizado para a verificação em duas etapas.

Configurar a verificação em duas etapas via SMS

Para configurar a verificação em duas etapas via SMS:

1. No Kaspersky Security Center Cloud Console, clique no link com o nome da conta e selecione **Gerenciar a conta de usuário**.

   A janela **Configurações da conta de usuário** é aberta.

2. Selecione a seção **Verificação em duas etapas**.

3. Clique no botão **configurar**.

4. Em **Digite sua senha atual**, especifique a senha da conta no Kaspersky Security Center Cloud Console e, em seguida, clique no botão **Continuar**.

5. Em **especificar o número do celular**, indique o número do aparelho que você deseja utilizar na verificação em duas etapas e depois clique no botão **próximo**.

   > É possível utilizar o mesmo número de telefone para até cinco contas.

   Um código de segurança de 6 dígitos será enviado para o número de telefone especificado.

6. Em **Confirme seu número de telefone**, digite o código de segurança recebido.

A verificação em duas etapas está configurada. Agora, toda vez que entrar com seu endereço de e-mail e senha, ou caso esqueça sua senha, será necessário digitar um código de segurança único recebido via SMS no número de telefone especificado.

Agora você pode instalar e configurar um aplicativo autenticador, alterar o número do telefone ou desativar a verificação em duas etapas.

Configurar a verificação em duas etapas usando um aplicativo autenticador

Os aplicativos autenticadores não podem ser utilizados no Kaspersky Security Center Cloud Console como um método autônomo de verificação. Primeiro, configure a verificação em duas etapas via SMS. Ao desativar a verificação em duas etapas por meio de seu número de celular, a verificação pelo aplicativo autenticador é desligada automaticamente. Após configurar as verificações via SMS e via aplicativo, será possível selecionar um método de verificação na página de acesso ou caso esqueça sua senha.

Para configurar a verificação em duas etapas por um aplicativo autenticador:

1. Configurar a verificação em duas etapas via SMS.

2. Faça o download, instale e execute o aplicativo autenticador que deseja utilizar.

   Nós testamos apenas o Google Authenticator e o Microsoft Authenticator para verificar a compatibilidade com o Kaspersky Security Center Cloud Console, e esses aplicativos eram gratuitos na época. As interfaces dos aplicativos podem não estar disponíveis no idioma de preferência. Verifique também a conformidade com a GDPR e as políticas de privacidade antes de usar os aplicativos. A Kaspersky não é de forma alguma patrocinada, apoiada ou afiliada a qualquer um dos proprietários desses aplicativos.

   > O Microsoft Authenticator pode ser instalado apenas em dispositivos móveis.

   Caso deseje, é possível usar outros aplicativos por sua própria conta e risco. O aplicativo usado deve ser compatível com códigos de segurança de 6 dígitos.

   Também recomendamos instalar um aplicativo autenticador em um dispositivo que não seja o celular. Dessa forma, será possível entrar em sua conta se o celular for perdido ou roubado.

3. No Kaspersky Security Center Cloud Console, clique no link com o nome da conta e selecione **Gerenciar a conta de usuário**.

   A janela **Configurações da conta de usuário** é aberta.

4. Selecione a seção **Verificação em duas etapas**.

5. Clique no botão **obter chave secreta**.

6. Em **Digite sua senha atual**, especifique a senha da conta no Kaspersky Security Center Cloud Console e, em seguida, clique no botão **Continuar**.

   A página do portal exibe uma chave secreta de 16 caracteres e um código QR.

7. No aplicativo autenticador de cada dispositivo, crie uma conta e digite a chave secreta exibida. Como alternativa, é possível verificar o código QR com o celular. Nesse caso, a conta será criada automaticamente. Consulte a documentação do aplicativo para saber mais informações.

   Um código de segurança de 6 dígitos é gerado em seus aplicativos autenticadores.

8. Verifique se os códigos de segurança gerados em seus aplicativos são os mesmos em cada dispositivo.

9. No Kaspersky Security Center Cloud Console, digite o código de segurança gerado.

A verificação em duas etapas por um aplicativo autenticador está configurada. Agora, toda vez que você entrar com seu endereço de e-mail e senha, ou caso esqueça a senha, será necessário digitar um código de segurança único gerado em seu aplicativo autenticador.

Agora é possível desativar o uso de um aplicativo autenticador ou desativar completamente a verificação em duas etapas.

Alterar o número do celular

Para alterar o número do celular utilizado na verificação em duas etapas via SMS:

1. No Kaspersky Security Center Cloud Console, clique no link com o nome da conta e selecione **Gerenciar a conta de usuário**.

   A janela **Configurações da conta de usuário** é aberta.

2. Selecione a seção **Verificação em duas etapas**.

3. Em **número de telefone**, clique no link **alterar número de telefone**.

4. Em **especificar o número de celular**, especifique o novo número que você deseja utilizar na verificação em duas etapas, em seguida, clique no botão **próximo**.

5. Em **Digite sua senha atual**, especifique a senha da conta no Kaspersky Security Center Cloud Console e, em seguida, clique no botão **Continuar**.

   Um código de segurança de 6 dígitos será enviado para o número de telefone especificado.

6. Em **Confirme seu número de telefone**, digite o código de segurança recebido.

O número de telefone celular foi alterado. Agora, os códigos de segurança únicos serão enviados para o novo número de telefone.

Desativar a verificação em duas etapas

Se não quiser mais utilizar a verificação em duas etapas, é possível desativá-la, conforme descrito nesta seção.

A desativação da verificação em duas etapas diminuirá a segurança de sua conta. Recomendamos veementemente que você continue utilizando a verificação em duas etapas.

Se tiver configurado a verificação em duas etapas via SMS, é possível desativar a verificação em duas etapas. Se tiver configurado a verificação em duas etapas por um aplicativo autenticador, é possível desativar o uso do aplicativo ou a verificação em duas etapas.

Para desativar o uso de um aplicativo autenticador:

1. No Kaspersky Security Center Cloud Console, clique no link com o nome da conta e selecione **Gerenciar a conta de usuário**.

   A janela **Configurações da conta de usuário** é aberta.

2. Selecione a seção **Verificação em duas etapas**.

3. Em **aplicativo autenticador**, clique no link **desativar o uso do aplicativo autenticador**.

4. Em **Digite sua senha atual**, especifique a senha da conta no Kaspersky Security Center Cloud Console e, em seguida, clique no botão **Continuar**.

O uso do aplicativo autenticador é desativado. As configurações de verificação em duas etapas por um aplicativo autenticador são excluídas. Agora é possível excluir as contas nos aplicativos autenticadores.

Posteriormente, você poderá configurar a verificação em duas etapas por um aplicativo autenticador novamente.

Para desativar completamente a verificação em duas etapas:

1. No Kaspersky Security Center Cloud Console, clique no link com o nome da conta e selecione **Gerenciar a conta de usuário**.

   A janela **Configurações da conta de usuário** é aberta.

2. Selecione a seção **Verificação em duas etapas**.

3. Em **número de telefone**, clique no link **desativar verificação em duas etapas**.

4. Em **Digite sua senha atual**, especifique a senha da conta no Kaspersky Security Center Cloud Console e, em seguida, clique no botão **Continuar**.

A verificação em duas etapas é desabilitada. Se você usava a verificação em duas etapas por um aplicativo autenticador, as configurações de verificação em duas etapas serão excluídas. Agora é possível excluir as contas nos aplicativos autenticadores.

Posteriormente, você poderá configurar a verificação em duas etapas novamente.

Excluir uma conta no Kaspersky Security Center Cloud Console

Se quiser parar de usar o Kaspersky Security Center Cloud Console, poderá excluir sua conta.

Ao excluir uma conta, todos os dados associados a ela são perdidos.

Depois de excluir a conta, não será mais possível acessar os espaços de trabalho no Kaspersky Endpoint Security Cloud, Kaspersky Security for Microsoft Office 365 e Kaspersky Security Center Cloud Console. Se você for o único administrador em um espaço de trabalho, ele será devidamente excluído. Além disso, o acesso à conta My Kaspersky será perdido.

Para excluir uma conta no Kaspersky Security Center Cloud Console:

1. No Kaspersky Security Center Cloud Console, clique no link com o nome da conta e selecione **Gerenciar a conta de usuário**.

   A janela **Configurações da conta de usuário** é aberta.

2. Selecione a seção **Excluir a conta de usuário**.

   A seção **Excluir conta de usuário** exibe informações sobre as consequências da exclusão da conta e, abaixo delas, o botão **Excluir**.

3. Leia as informações sobre a exclusão da conta e clique no botão **Excluir**.

   A janela **Insira a senha da sua conta de usuário** é aberta.

4. No campo de entrada de senha, digite a senha e clique no botão **Continuar.**

Sua conta é excluída.

Selecionando os data centers usados para armazenar informações do Kaspersky Security Center Cloud Console

Um espaço de trabalho do Kaspersky Security Center Cloud Console é criado usando servidores de uma rede de Data Centers globais baseados na plataforma na nuvem do Microsoft Azure. A seleção de Data Centers para hospedar um espaço de trabalho depende do país especificado ao registrá-lo no Kaspersky Security Center Cloud Console (consulte a tabela abaixo). Os pacotes de distribuição de aplicativos de segurança estão hospedados nos mesmos servidores das áreas de trabalho.

Correspondência da localização da empresa com uma região do Microsoft Azure

O país no qual em a empresa está localizada	Região do data center da Microsoft
Argentina	Brasil Sul
Bolívia	Brasil Sul
Brasil	Brasil Sul
Chile	Brasil Sul
Colômbia	Brasil Sul
Equador	Brasil Sul
Guiana	Brasil Sul
Peru	Brasil Sul
Paraguai	Brasil Sul
Suriname	Brasil Sul
Uruguai	Brasil Sul
Venezuela	Brasil Sul
Antígua e Barbuda	Leste dos EUA
Anguilla	Leste dos EUA
Aruba	Leste dos EUA
Barbados	Leste dos EUA
São Bartolomeu	Leste dos EUA
Bonaire, Santo Eustáquio e Saba	Leste dos EUA
Belize	Leste dos EUA
Costa Rica	Leste dos EUA
Cuba	Leste dos EUA
Curaçao	Leste dos EUA
Dominica	Leste dos EUA
República Dominicana	Leste dos EUA
Granada	Leste dos EUA
Guadalupe	Leste dos EUA
Guatemala	Leste dos EUA

Honduras	Leste dos EUA
Haiti	Leste dos EUA
Jamaica	Leste dos EUA
São Cristóvão e Nevis	Leste dos EUA
Ilhas Caimã	Leste dos EUA
Santa Lúcia	Leste dos EUA
São Martinho	Leste dos EUA
Martinica	Leste dos EUA
Montserrat	Leste dos EUA
Nicarágua	Leste dos EUA
Panamá	Leste dos EUA
Porto Rico	Leste dos EUA
Sint Maarten	Leste dos EUA
Trindade e Tobago	Leste dos EUA
São Vicente e Granadinas	Leste dos EUA
Ilhas Virgens Britânicas	Leste dos EUA
Ilhas Virgens Americanas	Leste dos EUA
Japão	Leste dos EUA
Canadá (New Brunswick)	Leste dos EUA
Canadá (Newfoundland e Labrador)	Leste dos EUA
Canadá (Nova Escotia)	Leste dos EUA
Canadá (Ontário)	Leste dos EUA
Canadá (Ilha do Príncipe Eduardo)	Leste dos EUA
Canadá (Quebec)	Leste dos EUA
Estados Unidos da América (Alabama)	Leste dos EUA
Estados Unidos da América (Arkansas)	Leste dos EUA
Estados Unidos da América (Connecticut)	Leste dos EUA
Estados Unidos da América (Distrito de Columbia)	Leste dos EUA
Estados Unidos da América (Delaware)	Leste dos EUA
Estados Unidos da América (Flórida)	Leste dos EUA
Estados Unidos da América (Geórgia)	Leste dos EUA
Estados Unidos da América (Iowa)	Leste dos EUA
Estados Unidos da América (Illinois)	Leste dos EUA
Estados Unidos da América (Indiana)	Leste dos EUA
Estados Unidos da América (Kentucky)	Leste dos EUA
Estados Unidos da América (Louisiana)	Leste dos EUA

Estados Unidos da América (Massachusetts)	Leste dos EUA
Estados Unidos da América (Maryland)	Leste dos EUA
Estados Unidos da América (Maine)	Leste dos EUA
Estados Unidos da América (Michigan)	Leste dos EUA
Estados Unidos da América (Minnesota)	Leste dos EUA
Estados Unidos da América (Missouri)	Leste dos EUA
Estados Unidos da América (Mississippi)	Leste dos EUA
Estados Unidos da América (Carolina do Norte)	Leste dos EUA
Estados Unidos da América (New Hampshire)	Leste dos EUA
Estados Unidos da América (Nova Jersey)	Leste dos EUA
Estados Unidos da América (Nova York)	Leste dos EUA
Estados Unidos da América (Ohio)	Leste dos EUA
Estados Unidos da América (Pensilvânia)	Leste dos EUA
Estados Unidos da América (Rhode Island)	Leste dos EUA
Estados Unidos da América (Carolina do Sul)	Leste dos EUA
Estados Unidos da América (Tennessee)	Leste dos EUA
Estados Unidos da América (Virgínia)	Leste dos EUA
Estados Unidos da América (Vermont)	Leste dos EUA
Estados Unidos da América (Wisconsin)	Leste dos EUA
Estados Unidos da América (Virgínia Ocidental)	Leste dos EUA
Albânia	Norte da Europa (Irlanda)
Bósnia e Herzegovina	Norte da Europa (Irlanda)
Bulgária	Norte da Europa (Irlanda)
Bielorrússia	Norte da Europa (Irlanda)
República Checa	Norte da Europa (Irlanda)
Dinamarca	Norte da Europa (Irlanda)
Estônia	Norte da Europa (Irlanda)
Finlândia	Norte da Europa (Irlanda)
Reino Unido	Norte da Europa (Irlanda)
Groelândia	Norte da Europa (Irlanda)
Grécia	Norte da Europa (Irlanda)
Croácia	Norte da Europa (Irlanda)
Hungria	Norte da Europa (Irlanda)
Irlanda	Norte da Europa (Irlanda)
Islândia	Norte da Europa (Irlanda)
Quirguistão	Norte da Europa (Irlanda)

Cazaquistão	Norte da Europa (Irlanda)
Lituânia	Norte da Europa (Irlanda)
Letônia	Norte da Europa (Irlanda)
Moldova	Norte da Europa (Irlanda)
Montenegro	Norte da Europa (Irlanda)
Macedônia	Norte da Europa (Irlanda)
Mongólia	Norte da Europa (Irlanda)
Noruega	Norte da Europa (Irlanda)
Polônia	Norte da Europa (Irlanda)
Romênia	Norte da Europa (Irlanda)
Sérvia	Norte da Europa (Irlanda)
Federação Russa	Norte da Europa (Irlanda)
Suécia	Norte da Europa (Irlanda)
Eslovênia	Norte da Europa (Irlanda)
Eslováquia	Norte da Europa (Irlanda)
Tajiquistão	Norte da Europa (Irlanda)
Turquemenistão	Norte da Europa (Irlanda)
Usbequistão	Norte da Europa (Irlanda)
Canadá (Alberta)	Oeste dos EUA
Canadá (Colúmbia Britânica)	Oeste dos EUA
Canadá (Manitoba)	Oeste dos EUA
Canadá (Territórios do Noroeste)	Oeste dos EUA
Canadá (Nunavut)	Oeste dos EUA
Canadá (Yukon)	Oeste dos EUA
Canadá (Saskatchewan)	Oeste dos EUA
México	Oeste dos EUA
Estados Unidos da América (Alasca)	Oeste dos EUA
Estados Unidos da América (Arizona)	Oeste dos EUA
Estados Unidos da América (Califórnia)	Oeste dos EUA
Estados Unidos da América (Colorado)	Oeste dos EUA
Estados Unidos da América (Havaí)	Oeste dos EUA
Estados Unidos da América (Idaho)	Oeste dos EUA
Estados Unidos da América (Kansas)	Oeste dos EUA
Estados Unidos da América (Montana)	Oeste dos EUA
Estados Unidos da América (Dakota do Norte)	Oeste dos EUA
Estados Unidos da América (Nebraska)	Oeste dos EUA

Estados Unidos da América (Novo México)	Oeste dos EUA
Estados Unidos da América (Nevada)	Oeste dos EUA
Estados Unidos da América (Oklahoma)	Oeste dos EUA
Estados Unidos da América (Oregon)	Oeste dos EUA
Estados Unidos da América (Dakota do Sul)	Oeste dos EUA
Estados Unidos da América (Texas)	Oeste dos EUA
Estados Unidos da América (Utah)	Oeste dos EUA
Estados Unidos da América (Washington)	Oeste dos EUA
Estados Unidos da América (Wyoming)	Oeste dos EUA
Estados Unidos da América (outras divisões administrativas)	Leste dos EUA
Outros países	Europa Ocidental (Holanda)

Acesso aos servidores DNS públicos

Caso o acesso aos servidores Kaspersky que usam o DNS do sistema não seja possível, o Kaspersky Security Center Cloud Console poderá usar estes servidores DNS públicos na seguinte ordem:

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

As solicitações para esses servidores DNS podem conter endereços de domínio e o endereço IP público de dispositivos cliente, porque o agente de rede estabelece uma conexão TCP/UDP com o servidor DNS. Caso o Kaspersky Security Center Cloud Console esteja usando um Servidor DNS público, o processamento de dados será regido pela Política de Privacidade do serviço pertinente.

Cenário: criação de uma hierarquia de Servidores de Administração gerenciados no Kaspersky Security Center Cloud Console

Este cenário descreve as ações que você deve executar para criar uma hierarquia de Servidores de Administração gerenciados no Kaspersky Security Center Cloud Console, que assume a função de Servidor de Administração principal. Essa hierarquia pode ser usada posteriormente para a migração de dispositivos e objetos gerenciados do Kaspersky Security Center para o Kaspersky Security Center Cloud Console, além do gerenciamento de Servidores de Administração e dispositivos secundários por meio do Kaspersky Security Center Cloud Console.

O Kaspersky Security Center Cloud Console pode atuar apenas como Servidor de Administração principal e os Servidores de Administração em execução no local podem atuar somente como Servidores de Administração secundários. Outros esquemas hierárquicos não estão disponíveis.

Pré-requisitos

Antes de iniciar, verifique se os seguintes pré-requisitos foram atendidos:

- Upgrade do Servidor de Administração em execução no local para a versão 12 ou posterior.
- Instalação do Kaspersky Security Center Web Console no Servidor de Administração em execução no local.
- Instalação dos plug-ins da Web para os aplicativos que você pretende gerenciar através do Kaspersky Security Center Cloud Console.
- Atualização dos aplicativos gerenciados para as versões compatíveis com o Kaspersky Security Center Cloud Console.
- Certifique-se de que a tarefa Baixar atualizações no repositório do Servidor de Administração no Servidor de Administração em execução no local não tenha o Servidor de Administração principal atribuído como a fonte de atualização. Se necessário, modifique as configurações da tarefa em conformidade.

Após a criação da hierarquia, as políticas e tarefas ativas no Kaspersky Security Center Cloud Console são aplicadas no Servidor de Administração secundário, substituindo assim as políticas e tarefas existentes. Caso queira evitar esse comportamento, exclua todas as políticas e tarefas do Kaspersky Security Center Cloud Console antes da criação da hierarquia. Como alternativa, é possível alterar o status de cada política do Kaspersky Security Center Cloud Console para **Inativo** nas configurações da política e desativar a opção **Distribuir em Servidores de Administração secundários e virtuais** nas configurações de cada tarefa do Kaspersky Security Center Cloud Console.

Você pode excluir sua hierarquia de Servidores de Administração a qualquer momento, se necessário.

Etapas da criação da hierarquia

O cenário básico fornece um Servidor de Administração secundário que não pode ser acessado pela Internet. No entanto, o conjunto de ações em algumas dos passos descritos abaixo pode variar se o Servidor de Administração secundário for acessível pela Internet. Além disso, nesse caso, alguns dos passos devem ser ignorados.

A criação de uma hierarquia de Servidores de Administração compreende as seguintes etapas:

1. **Recuperação do certificado do Servidor de Administração secundário**

   Se o Servidor de Administração secundário for acessível pela Internet, ignore este passo.

   No Kaspersky Security Center Web Console em execução local, abra as propriedades do Servidor de Administração e, na guia **Geral**, abra a seção **Geral**. Clique no link **Exibir certificado do Servidor de Administração**. O arquivo do certificado, no formato CER, é salvo automaticamente na pasta especificada nas configurações do seu navegador.

2. **Recuperação das configurações de conexão e dos certificados do Kaspersky Security Center Cloud Console**

   Se o Servidor de Administração secundário for acessível pela Internet, ignore este passo.

   No Kaspersky Security Center Cloud Console, abra as propriedades do Servidor de Administração e, na guia **Geral**, abra a seção **Hierarquia de Servidores de Administração**. As seguintes configurações de conexão são exibidas:

   - Endereço HDS

     Exibe o endereço da Web usado para a conexão ao Hosted Discovery Service (HDS).

   - Porta HDS

     Exibe o número da porta usada para a conexão ao HDS.

   A seção também contém dois links:

   - Exibir certificado do Servidor de Administração

     Clicar nesse link inicia o download da chave pública do certificado de instância do Kaspersky Security Center Cloud Console.

   - Certificado de CA Raiz HDS

     Clicar nesse link inicia o download do arquivo no formato .pem, que contém uma lista de certificados raiz confiáveis emitidos por autoridades de certificação (CA, Certificate Authorities). Esse arquivo foi projetado para uso pelo Servidor de Administração secundário: ele é necessário para verificar o certificado HDS.

   Copie as configurações de conexão manualmente, usando a área de transferência ou qualquer outra maneira conveniente, e salve-as em um arquivo de qualquer formato acessível. Clique no link **Exibir certificado do Servidor de Administração** e aguarde até que o arquivo do certificado seja baixado. Clique no link **Certificado de CA Raiz HDS** e aguarde até que o arquivo com a lista de certificados raiz confiáveis emitidos por autoridades de certificação seja baixado. Ambos os arquivos são salvos na pasta especificada nas configurações do navegador.

3. **Selecionando o Servidor de Administração secundário para conexão**

Nas propriedades do Servidor de Administração, prossiga para a guia **Servidores de administração**. Na hierarquia de grupos de administração, marque a caixa de seleção ao lado do grupo de administração que deseja que contenha o Servidor de Administração secundário com todos os seus dispositivos gerenciados. Clique no botão **Conectar Servidor de Administração secundário**.

Na página aberta, no campo **Nome de exibição do Servidor de Administração secundário**, especifique o nome com o qual o Servidor de Administração secundário deve ser exibido na hierarquia. Ele é usado apenas para sua conveniência e, portanto, pode ser diferente do nome real do Servidor de Administração secundário, se necessário. Clique em **Avançar**.

Se o Servidor de Administração secundário for acessível pela Internet, também será necessário especificar o endereço do Servidor de Administração secundário no campo **Endereço do Servidor de Administração secundário (opcional)**.

Na próxima página, clique no botão **Procurar** e especifique o arquivo .pem salvo no Servidor de Administração secundário. Clique em **Avançar**.

4. **Ativação e configuração do servidor proxy**

As ações descritas nesta etapa são opcionais. Execute-as somente se a conexão exigir o uso do servidor proxy.

Clique em **Avançar**. Na página **Definir como conectar o Servidor de Administração secundário ao Servidor de Administração principal**, você pode ativar e configurar o uso do servidor proxy, se necessário. Marque a caixa de seleção **Usar o servidor proxy** e especifique as seguintes configurações de proxy:

- Endereço

  O endereço do servidor proxy.

- Nome do usuário

  O nome de usuário usado para login no servidor proxy.

- Senha

  A senha usada para login no servidor proxy.

5. **Especificando as configurações de autenticação e inclusão do Servidor de Administração secundário na hierarquia**

Clique em **Avançar**. Na página **Credenciais do Servidor de Administração secundário**, especifique as seguintes configurações:

- Nome do usuário

  O nome de usuário usado para login no Servidor de Administração secundário.

- Senha

  A senha usada para login no Servidor de Administração secundário.

Clique em **Avançar** e aguarde até que o Servidor de Administração secundário seja exibido na hierarquia.

Se o Servidor de Administração secundário for acessível pela Internet, ele se conectará ao Servidor de Administração principal.

Se o Servidor de Administração secundário for acessível pela Internet e a conexão entre os dois Servidores de Administração for estabelecida com êxito, ignore todos os passos adicionais.

Se o Servidor de Administração Secundário não puder ser acessado pela Internet, ficará visível, mas você deverá executar ações adicionais no Servidor para controlá-lo.

6. **Configuração da conexão no Kaspersky Security Center Web Console em execução no local**

No Kaspersky Security Center Web Console em execução no local, abra as propriedades do Servidor de Administração e, na guia **Geral**, abra a seção **Hierarquia de Servidores de Administração**. Marque a caixa de seleção **Esse Servidor de Administração é secundário na hierarquia**. Na lista **Tipo do Servidor de Administração Principal**, selecione a opção **Kaspersky Security Center Cloud Console**.

O Kaspersky Security Center Web Console verifica se o Servidor de Administração principal está especificado como a fonte de atualização na tarefa *Baixar atualizações para o repositório do Servidor de Administração*. Se o Servidor de Administração principal for especificado como a fonte de atualização, você receberá a mensagem de aviso correspondente e um link para as configurações da tarefa. É possível modificar as configurações e voltar à criação da hierarquia ou ignorar essa ação e prosseguir com a criação da hierarquia.

No grupo **Configurações para estabelecer conexão entre Servidores de Administração secundário e principal**, especifique as seguintes configurações:

- Endereço do servidor HDS (do Servidor de Administração Principal no Cloud Console)

  Insira o endereço do servidor HDS no formato FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) que você copiou e salvou das propriedades do Servidor de Administração no Kaspersky Security Center Cloud Console.

- Portas do servidor HDS

  Insira os números da(s) porta(s) do servidor HDS que você copiou e salvou nas propriedades do Servidor de Administração no Kaspersky Security Center Cloud Console.

7. **Adicionando certificados ao Servidor de Administração secundário**

Clique no botão **Especifique o certificado do Servidor de Administração Principal** e especifique o arquivo do certificado salvo nas propriedades do Servidor de Administração no Kaspersky Security Center Cloud Console.

Clique no botão **Especifique os certificados do Serviço de Descoberta Hospedada** e especifique o arquivo .pem salvo nas propriedades do Servidor de Administração no Kaspersky Security Center Cloud Console.

Se você ativou o uso do servidor proxy ao conectar o Servidor de Administração secundário no Kaspersky Security Center Cloud Console, marque a caixa de seleção **Usar o servidor proxy** e especifique as mesmas configurações de proxy existentes no Kaspersky Security Center Cloud Console.

Também é possível marcar a caixa de seleção **Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ** se o Servidor de Administração secundário estiver em uma zona desmilitarizada (DMZ).

O Servidor de Administração secundário se conecta ao Servidor de Administração principal.

Resultados

Ao executar as etapas acima, verifique se a hierarquia foi criada com sucesso:

- As políticas ativas do Servidor de Administração principal entram em vigor no Servidor de Administração secundário. As tarefas do Servidor de Administração principal são distribuídas para o Servidor de Administração secundário. Se a opção **Distribuir em Servidores de Administração secundários e virtuais** estiver ativada nas configurações de uma tarefa de grupo, todas essas tarefas também serão distribuídas para o Servidor de Administração secundário.

- As configurações de política bloqueadas para alterações no Servidor de Administração principal são exibidas como bloqueadas para alterações em todas as políticas no Servidor de Administração secundário.

- As políticas aplicadas pelo Servidor de Administração principal são exibidas na lista de políticas do Servidor de Administração secundário (**Ativos (dispositivos)** → **Políticas e perfis**).

- As tarefas de grupo distribuídas pelo Servidor de Administração principal são exibidas na lista de tarefas do Servidor de Administração secundário (**Ativos (dispositivos)** → **Tarefas**).

- As políticas e tarefas criadas no servidor de administração principal não podem ser modificadas no servidor de administração secundário.

- No Kaspersky Security Center Cloud Console, na estrutura dos grupos de administração, o Servidor de Administração secundário é exibido dentro do grupo selecionado ao adicioná-lo.

Migração para o Kaspersky Security Center Cloud Console

Esta seção descreve o processo de migração para o Kaspersky Security Center Cloud Console a partir de:

- Kaspersky Security Center Web Console na versão 12 (ou posterior) em execução no local.
- Kaspersky Endpoint Security Cloud.

Métodos de migração para o Kaspersky Security Center Cloud Console

Usando o recurso de migração, é possível transferir seus dispositivos de rede do Kaspersky Security Center gerenciado pelo Kaspersky Security Center Cloud Console. Seus dispositivos gerenciados serão alternados sem perder as configurações principais, como associação a grupos de administração, bem como os objetos essenciais, como políticas e tarefas, relacionados aos aplicativos gerenciados.

Você pode escolher um dos dois métodos disponíveis para migrar seus Servidores de Administração para o Kaspersky Security Center Cloud Console:

- Migração sem uma hierarquia de Servidores de Administração:
  - Permite a transferência de dispositivos gerenciados e objetos relacionados para o Kaspersky Security Center Cloud Console, mesmo que o Servidor de Administração local não seja secundário em relação ao Kaspersky Security Center Cloud Console.
  - Pode exigir a transferência de arquivos (em uma unidade removível, por e-mail, por pastas compartilhadas ou de qualquer outra maneira conveniente) se o Kaspersky Security Center Web Console e o Kaspersky Security Center Cloud Console estiverem abertos em dispositivos físicos diferentes.

  Você também pode realizar a migração com Servidores de Administração virtuais se a sua rede os incluir.

- Migração usando uma hierarquia de Servidores de Administração:
  - Permite a transferência de dispositivos gerenciados e objetos relacionados para o Kaspersky Security Center Cloud Console usando apenas a interface do Kaspersky Security Center Cloud Console, de modo que nenhuma transferência física de arquivos seja necessária.
  - Requer que o Servidor de Administração executado no local atue como secundário do Kaspersky Security Center Cloud Console. É possível criar essa hierarquia antes de iniciar a migração.

Para a criptografia completa do disco, o Kaspersky Security Center Cloud Console é compatível apenas com o BitLocker.

Cenário: migração sem uma hierarquia de Servidores de Administração

Esta seção descreve a migração dos dispositivos gerenciados e objetos relacionados (como políticas, tarefas e relatórios) do Kaspersky Security Center Web Console em execução no local para o Kaspersky Security Center Cloud Console. É possível incluir um único grupo de administração no escopo da migração para restaurar o mesmo grupo de administração no Kaspersky Security Center Cloud Console.

Este grupo deve conter os dispositivos gerenciados de um único sistema operacional. Caso sua rede inclua dispositivos de diferentes sistemas operacionais ou distribuidores Linux, aloque-os em grupos de administração diferentes e, em seguida, migre cada grupo separadamente.

Após a conclusão da migração, todos os Agentes de Rede no escopo da migração são atualizados e gerenciados pelo Kaspersky Security Center Cloud Console.

As etapas listadas nesta seção abordam o processo de migração executado quando não existe uma hierarquia de Servidores de Administração, ou seja, nenhuma conexão foi estabelecida entre o Kaspersky Security Center Cloud Console e o Kaspersky Security Center Web Console executado localmente.

Pré-requisitos

Antes de começar, faça o seguinte:

- Atualizar o Servidor de Administração em execução no local para a seguinte versão:
  - Para dispositivos Windows – versão 12 ou posterior
  - Para dispositivos Linux – versão 12 Patch A ou posterior
- Instale o Kaspersky Security Center Web Console da versão 12.1 ou posterior.
- Atualize o Agente de Rede nos dispositivos gerenciados para a versão 12 ou posterior.
- Em dispositivos Windows, utilize o Agente de Rede sem uma senha de desinstalação.

  Caso a senha já tenha sido definida, execute um dos seguintes procedimentos no Kaspersky Security Center Web Console:
  - Desative a opção **Usar senha de desinstalação** nas configurações de política do Agente de rede.
  - Desinstale o Agente de Rede remotamente utilizando a tarefa *Desinstalar aplicativo remotamente*. No campo **Aplicativo a ser desinstalado** da tarefa, selecione o Agente de Rede do Kaspersky Security Center. Não se esqueça de inserir a senha de desinstalação.
- Atualize os aplicativos gerenciados para as versões compatíveis com o Kaspersky Security Center Cloud Console.
- Certifique-se de ter políticas para as versões mais recentes dos aplicativos gerenciados. Caso as políticas desatualizadas sejam utilizadas, crie novas políticas para as versões de aplicativos compatíveis com o Kaspersky Security Center Cloud Console.
- Para utilizar as políticas atuais, atualize os plug-ins da web para os aplicativos que pretende gerenciar por meio do Kaspersky Security Center Cloud Console.
- Desinstale os aplicativos da Kaspersky dos dispositivos gerenciados caso os aplicativos não sejam compatíveis com o Kaspersky Security Center Cloud Console e, em seguida, substitua os aplicativos desinstalados por outros compatíveis.
- Descriptografe todos os dados (no nível do disco ou do arquivo) que foram criptografados pelo Kaspersky Endpoint Security for Windows em dispositivos gerenciados executando o sistema operacional Windows e desative o recurso de criptografia nos dispositivos gerenciados por meio da política do aplicativo ou localmente. Para obter mais informações, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

Caso o dispositivo Windows ainda armazene quaisquer arquivos ou pastas criptografados pelo Kaspersky Endpoint Security for Windows, a atualização do Agente de Rede será cancelada durante o processo de migração. Uma notificação solicitará que você decifre todos os dados no dispositivo e desative o recurso de criptografia.

O Kaspersky Security Center Cloud Console permite no máximo 25.000 dispositivos gerenciados por Servidor de Administração.

Estágios da migração

A migração para o Kaspersky Security Center Cloud Console inclui as seguintes etapas:

1. **Planejando o escopo da migração e verificando os prerrequisitos**

   Estime o escopo do processo de migração, ou seja, analise o grupo de administração a ser exportado e avalie o número de dispositivos gerenciados nele. Além disso, verifique se todas as atividades listadas como prerrequisitos de migração foram concluídas com sucesso.

2. **Exportando dispositivos, objetos e configurações gerenciados do Kaspersky Security Center Web Console**

   Use o Assistente de Migração do Kaspersky Security Center Web Console executado no local para exportar os dispositivos gerenciados juntamente com seus objetos.

   O tamanho máximo do arquivo de exportação é de 4 GB.

3. **Importando o arquivo de exportação para o Kaspersky Security Center Cloud Console**

   Transfira as informações sobre os dispositivos e objetos gerenciados para o Kaspersky Security Center Cloud Console. Para isso, use o Assistente de Migração do Kaspersky Security Center Cloud Console para importar o arquivo de exportação e criar um pacote de instalação independente do Agente de Rede.

4. **Reinstalando o Agente de Rede em dispositivos gerenciados**

   Volte ao Assistente de Migração no Kaspersky Security Center Web Console em execução no local para criar uma tarefa de instalação remota. Será possível usar essa tarefa (imediatamente ou posteriormente) para reinstalar o Agente de Rede em seus dispositivos gerenciados e concluir o processo de migração.

Resultados

Ao concluir a migração, você pode conferir se ela deu certo:

- O Agente de Rede é reinstalado em todos os dispositivos gerenciados.
- Todos os dispositivos são gerenciados pelo Kaspersky Security Center Cloud Console.
- Todas as configurações de objeto em vigor antes da migração serão preservadas.

Assistente de migração

Esta seção fornece informações sobre o assistente de Migração no Kaspersky Security Center Cloud Console e no Kaspersky Security Center Web Console versão 12 ou posterior.

Etapa 1. Exportando dispositivos, objetos e configurações gerenciados do Kaspersky Security Center Web Console

A migração de dispositivos gerenciados do Kaspersky Security Center Web Console para o Kaspersky Security Center Cloud Console requer que você primeiro crie um arquivo de exportação contendo informações sobre a hierarquia de grupos de administração que estão no Servidor de Administração em execução atualmente no local. O arquivo de exportação também deve conter informações sobre os objetos e suas configurações. O arquivo de exportação será usado para a subsequente importação para o Kaspersky Security Center Cloud Console.

O tamanho máximo do arquivo de exportação é de 4 GB.

Para exportar objetos e suas configurações do Kaspersky Security Center Web Console:

1. No menu principal do Kaspersky Security Center Web Console, vá para **Operações** → **Migração**.
2. Na página de boas-vindas do assistente de Migração, clique em **Avançar**. A página **Dispositivos gerenciados para exportar** é aberta, exibindo toda a hierarquia de grupos de administração do Servidor de Administração correspondente.
3. Na página **Dispositivos gerenciados para exportar**, clique no ícone de chevron (>) próximo ao nome do grupo de **Dispositivos gerenciados** para expandir a hierarquia de grupos de administração. Selecione o grupo de administração que deseja exportar.

   Após a migração do Kaspersky Security Center em execução no local para o console do Kaspersky Security Center Cloud Console realizada para dois grupos de administração, as tarefas de instalação remota para esses grupos aparecem com o mesmo nome.

4. Selecione os aplicativos gerenciados cujas políticas e tarefas devem ser transferidas para o Kaspersky Security Center Cloud Console junto com os objetos de grupo. Para selecionar os aplicativos gerenciados cujos objetos devem ser exportados, marque as caixas de seleção ao lado de seus nomes na lista.

   Embora o Servidor de Administração do Kaspersky Security Center esteja presente na lista, marcar a caixa de seleção correspondente não resulta na exportação de suas políticas.

   Para certificar-se de que seus aplicativos gerenciados são compatíveis com o Kaspersky Security Center Cloud Console, clique no link correspondente. Isso redirecionará para o tópico da Ajuda Online que contém a lista de aplicativos gerenciados pelo Kaspersky Security Center Cloud Console.

   Ao selecionar aplicativos sem suporte no Kaspersky Security Center Cloud Console, as políticas e tarefas desses aplicativos ainda serão exportadas e depois importadas, mas não será possível gerenciá-las no Kaspersky Security Center Cloud Console devido à indisponibilidade dos plugins dedicados.

5. Visualize a lista de objetos de grupo exportados por padrão e especifique objetos que não sejam de grupos para serem exportados junto com o grupo de administração selecionado, se necessário. Configure o escopo da exportação incluindo ou excluindo vários objetos, como tarefas globais, seleções de dispositivos personalizadas, relatórios, funções personalizadas, usuários e grupos de segurança internos e categorias de aplicativos personalizadas. Esta página inclui as seguintes seções:

- **Tarefas globais**

  A lista de tarefas globais de aplicativos gerenciados, bem como tarefas globais do Agente de Rede.

  Se uma tarefa global selecionada se aplicar a uma seleção específica de objetos, essa seleção também será exportada.

  Embora as tarefas globais do Servidor de Administração estejam presentes na lista, você não pode exportá-las; selecionar essas tarefas não afeta o escopo da exportação. As tarefas de instalação remota também permanecem fora do escopo de exportação, porque seus respectivos pacotes de instalação não podem ser exportados.

- **Seleções de dispositivos**

  A lista de seleções de dispositivos personalizadas.

- **Relatórios**

  A lista editável de instâncias de relatório a serem exportadas.

  Se um relatório selecionado se aplicar a uma seleção específica de objetos, essa seleção também será exportada.

  O Kaspersky Security Center Cloud Console contém o mesmo conjunto de modelos de relatório do Kaspersky Security Center Web Console, portanto, você pode selecionar para exportar apenas os relatórios que criou manualmente ou reconfigurou.

- **Objetos de grupo**

A lista de objetos de grupo a serem exportados por padrão. Por padrão, os seguintes objetos relacionados ao grupo de administração selecionado serão exportados por inteiro:

- Estrutura do grupo de administração, ou seja, todos os subgrupos do grupo de administração selecionado
- Dispositivos incluídos nos grupos de administração a serem exportados
- Tags atribuídas aos dispositivos a serem exportados

  Se uma tag foi criada no Kaspersky Security Center Web Console, mas nunca foi atribuída a qualquer dispositivo, ela não será exportada. As regras de identificação automática também não serão exportadas.

- Políticas de grupo dos aplicativos gerenciados que foram selecionados

  As políticas do Servidor de Administração e do Agente de Rede não são exportadas.

- Tarefas de grupo dos aplicativos gerenciados selecionados e tarefas de grupo do Agente de Rede

  As tarefas do Servidor de Administração não são exportadas.

Também é possível impedir que certos tipos de objetos não pertencentes a grupos sejam exportados:

- Para cancelar a exportação de funções personalizadas (ou seja, aquelas criadas apenas pelo usuário), marque a caixa de seleção **Excluir funções personalizadas da exportação**.
- Para cancelar a exportação de usuários e grupos de segurança internos, marque a caixa de seleção **Excluir usuários internos e grupos de segurança da exportação**.
- Para cancelar a exportação de categorias de aplicativos personalizadas com conteúdo adicionado manualmente, marque a caixa de seleção **Excluir categorias de aplicativos personalizadas da exportação**.

Caso dispositivos de vários sistemas operacionais sejam transferidos para o Kaspersky Security Center Cloud Console, os objetos não pertencentes a grupos precisam ser migrados apenas uma vez.

O Assistente de Migração verifica o número total de dispositivos gerenciados incluídos no grupo de administração selecionado. Caso o número exceda 10.000, uma mensagem de erro será exibida. O botão **Avançar** permanece indisponível (esmaecido) até que o número de dispositivos gerenciados no grupo de administração selecionado reduza para um valor dentro do limite.

6. Depois de definir o escopo da migração, clique em **Avançar** para iniciar o processo de exportação. A página **Criando o arquivo de exportação** é aberta e é possível visualizar o progresso da exportação para cada tipo de objeto incluído no escopo da migração. Aguarde até que os ícones de atualização (🔄) ao lado de todos os itens na lista de objetos sejam substituídos por marcas de seleção verdes (✓). O processo de exportação termina e o arquivo de exportação é baixado automaticamente para o local padrão de download definido nas configurações do seu navegador. O nome do arquivo de exportação aparece na parte inferior da janela do navegador.

7. Quando a página **A exportação foi concluída com êxito** for exibida, prossiga para a próxima etapa executada no Kaspersky Security Center Cloud Console.

Caso você use o Kaspersky Security Center Web Console e o Kaspersky Security Center Cloud Console em dispositivos diferentes, será necessário copiar o arquivo de exportação para uma unidade removível ou escolher outras maneiras de transferir o arquivo.

Etapa 2. Importando o arquivo de exportação para o Kaspersky Security Center Cloud Console

Para transferir informações sobre dispositivos gerenciados, objetos e suas configurações exportadas do Kaspersky Security Center Web Console, é necessário importá-las para o Kaspersky Security Center Cloud Console implementado em seu espaço de trabalho. Isto permite criar um pacote de instalação independente e usá-lo para reinstalar o Agente de Rede nos dispositivos gerenciados.

Antes de iniciar o assistente de Migração no Kaspersky Security Center Cloud Console, certifique-se de que seu idioma de localização atual seja o mesmo do Kaspersky Security Center Web Console durante o processo de exportação. Mude o idioma, se necessário.

Caso já tenha concluído o assistente de início rápido no espaço de trabalho do Kaspersky Security Center Cloud Console, o grupo de **Dispositivos gerenciados** incluirá políticas e tarefas criadas com as configurações padrão. Exclua essas políticas e tarefas antes de importar aquelas exportadas do Kaspersky Security Center Web Console.

Para importar o arquivo de exportação para o Kaspersky Security Center Cloud Console:

1. Na janela principal do aplicativo Kaspersky Security Center Cloud Console, clique em **Operações** → **Migração**.
2. Na página de boas-vindas do Assistente de migração, clique em **Importar**. Na janela aberta do File Explorer, selecione o arquivo de exportação navegando até a pasta onde foi salvo e clique em **Abrir**. Aguarde até que o ícone de atualização (↻) ao lado do status de upload do arquivo seja substituído pela marca de seleção verde (✓).
3. Clique em **Avançar**. A próxima página é aberta, exibindo toda a hierarquia de grupos de administração do Servidor de Administração no Kaspersky Security Center Cloud Console.
4. Marque a caixa de seleção ao lado do grupo de administração de destino no qual os objetos de grupo devem ser restaurados e clique em **Avançar**. O assistente de Migração exibe uma lista de pacotes de instalação do Agente de Rede disponíveis no Kaspersky Security Center Cloud Console.
5. Selecione o pacote de instalação que contém a versão e a localização relevantes do Agente de Rede e clique em **Avançar**.

Selecione o pacote de instalação do Kaspersky Network Agent for Windows apenas se o Assistente de início rápido já tiver sido concluído no espaço de trabalho do Kaspersky Security Center Cloud Console, e se a migração dos dispositivos Windows for executada.

Aguarde até que o assistente de Migração crie um pacote de instalação independente. O tamanho máximo do arquivo do pacote de instalação independente para o Agente de Rede é de 200 MB.

O arquivo é descompactado e baixado automaticamente para o local padrão de download definido nas configurações do navegador. Os objetos não pertencentes a grupos e os objetos de grupos são restaurados para o grupo de administração de destino.

Quando a importação for concluída, a estrutura exportada dos grupos de administração, incluindo os detalhes dos dispositivos, aparecerá no grupo de administração de destino selecionado. Se o nome do objeto restaurado for idêntico ao nome de um objeto existente, será adicionado ao objeto restaurado um sufixo incremental.

Se você importou todo o grupo de **Dispositivos gerenciados**, recomendamos renomear o subgrupo recém-importado para evitar confusão:

a. Siga para a seção **Hierarquia de grupos**.

b. Clique no nome do subgrupo na árvore de grupos.

c. Na janela de propriedades que é aberta, no camp **Nome** insira um nome diferente (por exemplo, "Dispositivos migrados").

Recomendamos que você verifique se os objetos (políticas, tarefas e dispositivos gerenciados) incluídos no escopo de exportação foram importados com sucesso para o Kaspersky Security Center Cloud Console. Para fazer isso, vá para a seção **Ativos (dispositivos)** e verifique se os objetos importados aparecem nas listas nas subseções **Políticas e perfis**, **Tarefas**, e **Dispositivos gerenciados**.

Não é possível minimizar o assistente de Migração nem executar nenhuma operação simultânea durante a importação. Aguarde até que os ícones de atualização (↻) ao lado de todos os itens na lista de objetos sejam substituídos por marcas de seleção verdes (✓) e a importação será concluída. Em seguida, os dispositivos começam a mudar para o Kaspersky Security Center Cloud Console.

6. Clique em **Concluir** para fechar a janela do Assistente de migração.

7. Caso queira encontrar e baixar o pacote de instalação independente novamente, acesse **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação** e clique no botão **Exibir a lista de pacotes independentes**. Na lista aberta, selecione o pacote de instalação independente que você criou e clique no botão **Baixar**.

Caso você use o Kaspersky Security Center Web Console e o Kaspersky Security Center Cloud Console em dispositivos diferentes, será necessário copiar o pacote de instalação independente para uma unidade removível ou escolher outras maneiras de transferir o arquivo.

Etapa 3. Reinstalar o Agente de Rede nos dispositivos gerenciados pelo Kaspersky Security Center Cloud Console

Depois de criar o pacote de instalação independente do Agente de Rede, será possível prosseguir para a criação de uma tarefa de instalação remota. Executar esta tarefa permite reinstalar o Agente de Rede em todos os dispositivos gerenciados para que esses dispositivos sejam alternados sob o gerenciamento pelo Kaspersky Security Center Cloud Console.

Para reduzir o risco de perda de dados, recomendamos que você execute primeiro as ações para um pequeno grupo de administração com até 20 dispositivos gerenciados localizados na rede corporativa e sem servidores físicos. Depois de concluir essas ações, verifique se a reinstalação foi concluída com êxito e prossiga para o escopo de reinstalação completo.

Para criar uma tarefa de instalação remota e reinstalar o Agente de Rede:

1. Volte ao assistente de Migração no Kaspersky Security Center Web Console em execução no local.

   Recomendamos usar o assistente de migração para criar uma tarefa de instalação remota para reinstalar o Agente de rede conforme descrito abaixo. Caso seja necessário usar uma tarefa de instalação remota personalizada, em primeiro lugar, um pacote de instalação personalizada é preciso ser criado manualmente a partir do pacote de instalação independente do Agente de Rede. Observe que ao criar um pacote de instalação personalizado, é preciso especificar a chave "-s" na linha de comando do arquivo executável. Caso contrário, a reinstalação do Agente de Rede a partir do pacote de instalação personalizada será concluída com um erro.

   Dependendo do estado atual do assistente de Migração, é possível executar um dos seguintes procedimentos:

   - Caso não tenha fechado o Assistente de migração após a exportação e sua sessão não tiver expirado, clique no botão **Ir para a etapa 3 do assistente de migração**. Marque a caixa de seleção **Carregar pacote de instalação independente** e clique no botão **Selecionar pacote de instalação independente**. Na janela aberta do navegador, especifique o pacote de instalação independente do Agente de Rede.

   - Caso tenha que iniciar o Assistente de migração novamente por qualquer motivo, marque a caixa de seleção **Carregar pacote de instalação independente** e clique no botão **Selecionar pacote de instalação independente**. Na janela aberta do navegador, especifique o pacote de instalação independente do Agente de Rede. Depois disso, o assistente de Migração exibirá novamente a hierarquia de grupos de administração do Servidor de Administração. Selecione o mesmo grupo para o qual criou o arquivo de exportação e clique em **Avançar**.

     O assistente de Migração verifica novamente o número total de dispositivos gerenciados incluídos no grupo de administração selecionado. Caso o número exceda 10.000, uma mensagem de erro será exibida. O botão **Avançar** permanece indisponível (esmaecido) até que o número de dispositivos gerenciados no grupo de administração selecionado reduza para um valor dentro do limite.

2. Aguarde até que o pacote de instalação independente seja carregado e clique em **Avançar**. O assistente de Migração cria um pacote de instalação personalizado e uma tarefa de instalação remota para ele. O escopo da tarefa incluirá o grupo de administração selecionado na página **Dispositivos gerenciados para exportar**; o agendamento de inicialização da tarefa será definido para **Manualmente** por padrão. O assistente de Migração exibe o progresso da criação. Aguarde até que os ícones de atualização (🔄) sejam substituídos pelas marcas de seleção verdes (✓) e clique em **Avançar**.

3. Se necessário, marque a caixa de seleção **Executar tarefa de instalação remota recém-criada** (desmarcada por padrão) para os dispositivos no grupo de administração selecionado do Servidor de Administração em execução no local e todos os seus subgrupos. Nesse caso, os dispositivos serão trocados sob o gerenciamento do Kaspersky Security Center Cloud Console, mas somente após a instalação do Agente de Rede. Será exibido o caminho completo do grupo de administração no qual a tarefa será executada.

   A tarefa deve ser iniciada somente após a conclusão da importação para o Kaspersky Security Center Cloud Console. Caso contrário, os nomes dos dispositivos podem ser duplicados na lista.

4. Clique em **Concluir** para fechar o Assistente de migração e iniciar a tarefa de instalação remota para os seguintes fins:

   - Atualizar as instâncias do Agente de Rede
   - Alternar as instâncias do Agente de Rede sob gerenciamento pelo Kaspersky Security Center Cloud Console

   Caso tenha deixado a caixa de seleção **Executar tarefa de instalação remota recém-criada** desmarcada, é possível iniciar a tarefa manualmente mais tarde, se necessário.

É possível verificar se as instâncias do Agente de Rede migradas podem agora ser gerenciadas por meio do Kaspersky Security Center Cloud Console. Para fazer isso, acesse **Ativos (dispositivos)** → **Dispositivos gerenciados**. Certifique-se de que os dispositivos gerenciados migrados tenham o ícone de confirmação (✓) nas colunas **Visível**, **Agente de Rede instalado** e **Agente de Rede em execução**. Além disso, certifique-se de que os dispositivos não tenham a descrição do status *Não conectado há muito tempo*.

Migração com uma hierarquia de Servidores de Administração

Esta seção descreve a migração dos dispositivos gerenciados e objetos relacionados do Kaspersky Security Center Web Console executado localmente para o Kaspersky Security Center Cloud Console. O processo envolve uma hierarquia: o Kaspersky Security Center Web Console em execução no local atua como o servidor de administração secundário, e o Kaspersky Security Center Cloud Console atua como o Servidor de Administração principal.

Cada grupo de administração transferido para o Kaspersky Security Center Cloud Console deve conter os dispositivos gerenciados de um único sistema operacional. Caso sua rede inclua dispositivos de diferentes sistemas operacionais, aloque-os em grupos de administração diferentes e, em seguida, migre cada grupo separadamente.

Após a conclusão da migração, todos os Agentes de Rede do grupo no escopo da migração são atualizados e gerenciados através do Kaspersky Security Center Cloud Console.

Antes de começar, faça o seguinte:

- Atualizar o Servidor de Administração em execução no local para a seguinte versão:
  - Para dispositivos Windows – versão 12 ou posterior
  - Para dispositivos Linux – versão 12 Patch A ou posterior
- Instale o Kaspersky Security Center Web Console da versão 12.1 ou posterior.
- Atualize o Agente de Rede nos dispositivos gerenciados para a versão 12 ou posterior.
- Em dispositivos Windows, utilize o Agente de Rede sem uma senha de desinstalação.

  Caso a senha já tenha sido definida, execute um dos seguintes procedimentos no Kaspersky Security Center Web Console:

  - Desative a opção **Usar senha de desinstalação** nas configurações de política do Agente de rede.

- Desinstale o Agente de Rede remotamente utilizando a tarefa *Desinstalar aplicativo remotamente*. No campo **Aplicativo a ser desinstalado** da tarefa, selecione o Agente de Rede do Kaspersky Security Center. Não se esqueça de inserir a senha de desinstalação.

- Atualize os aplicativos gerenciados para as versões compatíveis com o Kaspersky Security Center Cloud Console.

- Certifique-se de ter políticas para as versões mais recentes dos aplicativos gerenciados. Caso as políticas desatualizadas sejam utilizadas, crie novas políticas para as versões de aplicativos compatíveis com o Kaspersky Security Center Cloud Console.

- Para utilizar as políticas atuais, atualize os plug-ins da web para os aplicativos que pretende gerenciar por meio do Kaspersky Security Center Cloud Console.

- Desinstale os aplicativos da Kaspersky dos dispositivos gerenciados caso os aplicativos não sejam compatíveis com o Kaspersky Security Center Cloud Console e, em seguida, substitua os aplicativos desinstalados por outros compatíveis.

- Descriptografe todos os dados (no nível do disco ou do arquivo) que foram criptografados pelo Kaspersky Endpoint Security for Windows em dispositivos gerenciados executando o sistema operacional Windows e desative o recurso de criptografia nos dispositivos gerenciados por meio da política do aplicativo ou localmente. Para obter mais informações, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

  Caso o dispositivo Windows ainda armazene quaisquer arquivos ou pastas criptografados pelo Kaspersky Endpoint Security for Windows, a atualização do Agente de Rede será cancelada durante o processo de migração. Uma notificação solicitará que você decifre todos os dados no dispositivo e desative o recurso de criptografia.

O Kaspersky Security Center Cloud Console permite no máximo 25.000 dispositivos gerenciados por Servidor de Administração.

Para executar a migração para o Kaspersky Security Center Cloud Console:

1. Estime o escopo do processo de migração, ou seja, analise o grupo de administração a ser exportado e avalie o número de dispositivos gerenciados nele. Verifique se todas as atividades listadas como pré-requisito de migração foram concluídas com sucesso.

2. No Kaspersky Security Center Cloud Console, acesse o Servidor de Administração secundário para os dispositivos gerenciados que deseja migrar.

3. No menu principal, acesse **Operações → Migração**.

   A página de boas-vindas do assistente de Migração é aberta.

4. Na página de boas-vindas, clique em **Avançar**.

   A página **Dispositivos gerenciados para exportar** é aberta, exibindo toda a hierarquia de grupos de administração do Servidor de administração secundário.

5. Na página **Dispositivos gerenciados para exportar**, clique no ícone de chevron (>) próximo ao nome do grupo **Dispositivos gerenciados** e expanda a hierarquia dos grupos de administração. Selecione o grupo de administração que deseja exportar.

O Assistente de Migração verifica o número total de dispositivos gerenciados incluídos no grupo de administração selecionado. Caso o número exceda 10.000, uma mensagem de erro será exibida. O botão **Avançar** permanece indisponível (esmaecido) até que o número de dispositivos gerenciados no grupo de administração selecionado reduza para um valor dentro do limite.

6. Selecione os aplicativos gerenciados cujas políticas e tarefas devem ser transferidas para o Kaspersky Security Center Cloud Console junto com os objetos de grupo. Para selecionar os aplicativos gerenciados cujos objetos devem ser exportados, marque as caixas de seleção ao lado de seus nomes na lista.

   Embora o Servidor de Administração do Kaspersky Security Center esteja presente na lista, marcar a caixa de seleção correspondente não resulta na exportação de suas políticas.

   Para certificar-se de que seus aplicativos gerenciados são compatíveis com o Kaspersky Security Center Cloud Console, clique no link correspondente. Isso redirecionará para o tópico da Ajuda Online que contém a lista de aplicativos gerenciados pelo Kaspersky Security Center Cloud Console.

   Ao selecionar aplicativos não compatíveis com o Kaspersky Security Center Cloud Console, as políticas e tarefas desses aplicativos ainda serão migradas, mas não será possível gerenciá-las no Kaspersky Security Center Cloud Console devido à indisponibilidade de plug-ins dedicados.

7. Visualize a lista de objetos de grupo exportados por padrão. Também é possível especificar objetos não pertencentes a grupos para serem exportados com o grupo de administração selecionado, se necessário, como tarefas globais, seleções de dispositivos personalizados, relatórios, funções personalizadas, usuários internos e grupos de segurança, bem como categorias de aplicativos personalizados com conteúdo adicionado manualmente. Esta página inclui as seguintes seções:

   - **Tarefas globais**

     A lista de tarefas globais de aplicativos gerenciados, bem como tarefas globais do Agente de Rede.

     Se uma tarefa global selecionada se aplicar a uma seleção específica de objetos, essa seleção também será exportada.

     Embora as tarefas globais do Servidor de Administração estejam presentes na lista, você não pode exportá-las; selecionar essas tarefas não afeta o escopo da exportação. As tarefas de instalação remota também permanecem fora do escopo de exportação, porque seus respectivos pacotes de instalação não podem ser exportados.

   - **Seleções de dispositivos**

     A lista de seleções de dispositivos personalizadas.

   - **Relatórios**

A lista editável de instâncias de relatório a serem exportadas.

Se um relatório selecionado se aplicar a uma seleção específica de objetos, essa seleção também será exportada.

O Kaspersky Security Center Cloud Console contém o mesmo conjunto de modelos de relatório do Kaspersky Security Center Web Console, portanto, você pode selecionar para exportar apenas os relatórios que criou manualmente ou reconfigurou.

- **Objetos de grupo**

A lista de objetos de grupo a serem exportados por padrão. Por padrão, os seguintes objetos relacionados ao grupo de administração selecionado serão exportados por inteiro:

- Estrutura do grupo de administração, ou seja, todos os subgrupos do grupo de administração selecionado
- Dispositivos incluídos nos grupos de administração a serem exportados
- Tags atribuídas aos dispositivos a serem exportados

  Se uma tag foi criada no Kaspersky Security Center Web Console, mas nunca foi atribuída a qualquer dispositivo, ela não será exportada. As regras de identificação automática também não serão exportadas.

- Políticas de grupo dos aplicativos gerenciados que foram selecionados

  As políticas do Servidor de Administração e do Agente de Rede não são exportadas.

- Tarefas de grupo dos aplicativos gerenciados selecionados e tarefas de grupo do Agente de Rede

  As tarefas do Servidor de Administração não são exportadas.

Também é possível impedir que certos tipos de objetos não pertencentes a grupos sejam exportados:

- Para cancelar a exportação de funções personalizadas (ou seja, aquelas criadas apenas pelo usuário), marque a caixa de seleção **Excluir funções personalizadas da exportação**.
- Para cancelar a exportação de usuários e grupos de segurança internos, marque a caixa de seleção **Excluir usuários internos e grupos de segurança da exportação**.
- Para cancelar a exportação de categorias de aplicativos personalizadas com conteúdo adicionado manualmente, marque a caixa de seleção **Excluir categorias de aplicativos personalizadas da exportação**.

Caso dispositivos de vários sistemas operacionais sejam transferidos para o Kaspersky Security Center Cloud Console, os objetos não pertencentes a grupos precisam ser migrados apenas uma vez.

8. Depois de definir o escopo da migração, clique em **Avançar** para iniciar o processo de exportação. A página **Criando o arquivo de exportação** é aberta e é possível visualizar o progresso da exportação para cada tipo de objeto incluído no escopo da migração. Aguarde até que os ícones de atualização (🔄) ao lado de cada item na lista de objetos sejam substituídos por uma marca de seleção verde (✓). A exportação termina e o arquivo de exportação é salvo automaticamente em uma pasta temporária. A próxima página é aberta, exibindo toda a hierarquia de grupos de administração no Kaspersky Security Center Cloud Console, que atua como o Servidor de administração principal.

9. Marque a caixa de seleção ao lado do grupo de administração para o qual os objetos de grupo devem ser importados e clique em **Avançar**. O arquivo é descompactado e os objetos do grupo e os objetos que não pertencem ao grupo são restaurados para o grupo de administração de destino.

   Se o nome do objeto restaurado for idêntico ao nome de um objeto existente, será adicionado ao objeto restaurado um sufixo incremental.

   Quando a importação for concluída, a estrutura exportada dos grupos de administração, incluindo os detalhes dos dispositivos, aparecerá no grupo de administração de destino selecionado. Os objetos não pertencentes a grupos também são importados.

   Não é possível minimizar o assistente de Migração nem executar nenhuma operação simultânea durante a importação. Aguarde até que os ícones de atualização (🔄) ao lado de cada item na lista de objetos sejam substituídos por uma marca de seleção verde (✓) e a importação seja concluída. Em seguida, os dispositivos começam a mudar para o Kaspersky Security Center Cloud Console.

10. Após a conclusão da importação, o Assistente de Migração exibe uma lista de pacotes de instalação do Agente de Rede disponíveis no Kaspersky Security Center Cloud Console para um sistema operacional apropriado. Selecione o pacote de instalação que contém a versão e a localização pertinentes do Agente de Rede.

    Selecione o pacote de instalação do Kaspersky Network Agent for Windows apenas se o Assistente de início rápido já tiver sido concluído no espaço de trabalho do Kaspersky Security Center Cloud Console, e se a migração dos dispositivos Windows for executada.

11. Clique em **Avançar**.

    O Assistente de Migração criará um novo pacote de instalação independente (ou usará um existente) e um pacote de instalação personalizada com base nele, além da tarefa de instalação remota correspondente. O escopo da tarefa inclui o grupo de administração selecionado na página **Dispositivos gerenciados para exportar**. O agendamento da inicialização da tarefa está definido para **Manualmente** por padrão. O assistente de Migração exibe o progresso da criação.

12. Aguarde até que os ícones de atualização (🔄) sejam substituídos por uma marca de seleção verde (✓) e clique em **Avançar**.

13. Se necessário, marque a caixa de seleção **Executar tarefa de instalação remota recém-criada** (desmarcada por padrão) para os dispositivos no grupo de administração selecionado no Kaspersky Security Center Web Console em execução no local e todos os seus subgrupos. Após a conclusão da instalação do Agente de Rede, é possível gerenciar os dispositivos selecionados por meio do Kaspersky Security Center Cloud Console. É exibido o caminho completo do grupo de administração no qual a tarefa deverá ser executada.

    A tarefa de instalação remota deve ser iniciada somente após a conclusão da importação para o Kaspersky Security Center Cloud Console. Caso contrário, os dispositivos podem ser duplicados.

14. Clique em **Concluir** para fechar o Assistente de migração e iniciar a tarefa de instalação remota para os seguintes fins:

    - Atualizar as instâncias do Agente de Rede
    - Gerenciar as instâncias do Agente de Rede pelo Kaspersky Security Center Cloud Console

    Caso tenha deixado a caixa de seleção **Executar tarefa de instalação remota** desmarcada, é possível iniciar a tarefa manualmente mais tarde, se necessário.

É possível verificar se as instâncias do Agente de Rede migradas podem agora ser gerenciadas por meio do Kaspersky Security Center Cloud Console. Para fazer isso, acesse **Ativos (dispositivos)** → **Dispositivos gerenciados**. Certifique-se de que os dispositivos gerenciados migrados tenham o ícone de confirmação (✓) nas colunas **Visível**, **Agente de Rede instalado** e **Agente de Rede em execução**. Além disso, certifique-se de que os dispositivos não tenham a descrição do status *Não conectado há muito tempo*.

Cenário: Migração de dispositivos executando sistemas operacionais Linux ou macOS

Esta seção descreve como fazer a migração dos dispositivos que executam os sistemas operacionais Linux ou macOS do Kaspersky Security Center Web Console executado localmente para o Kaspersky Security Center Cloud Console. Os cenários básicos de migração sem uma hierarquia de Servidores de Administração e migração com essa hierarquia permitem a transferência de todos os dispositivos e objetos relacionados para o Kaspersky Security Center Cloud Console. No entanto, caso sua rede inclua dispositivos que executam não apenas o Windows, mas também Linux ou macOS, será necessário transferir os dispositivos de cada tipo de sistema operacional separadamente. Consequentemente, é preciso realizar a migração várias vezes.

Pré-requisitos

Antes de começar, faça o seguinte:

- Atualize o Servidor de Administração em execução no local para a versão 12 Patch A ou posterior.
- Instale o Kaspersky Security Center Web Console na versão 12.1 ou posterior.
- Atualize o Agente de Rede em dispositivos gerenciados para a versão 12 ou posterior.
- Atualize os aplicativos gerenciados para as versões compatíveis com o Kaspersky Security Center Cloud Console.
- Certifique-se de ter políticas para as versões mais recentes dos aplicativos gerenciados. Caso as políticas desatualizadas sejam utilizadas, crie novas políticas para as versões de aplicativos compatíveis com o Kaspersky Security Center Cloud Console.
- Para utilizar as políticas atuais, atualize os plug-ins da web para os aplicativos que pretende gerenciar por meio do Kaspersky Security Center Cloud Console.
- Desinstale os aplicativos da Kaspersky dos dispositivos gerenciados caso os aplicativos não sejam compatíveis com o Kaspersky Security Center Cloud Console e, em seguida, substitua os aplicativos desinstalados por outros compatíveis.

O Kaspersky Security Center Cloud Console permite no máximo 25.000 dispositivos gerenciados por Servidor de Administração.

Estágios da migração

A migração para o Kaspersky Security Center Cloud Console inclui as seguintes etapas:

1. **Agrupamento de dispositivos gerenciados por seus sistemas operacionais**

   Se sua rede incluir dispositivos que executam sistemas operacionais diferentes (Windows, Linux ou macOS), coloque os dispositivos de cada sistema operacional em grupos de administração separados no Kaspersky Security Center Web Console. Além disso, crie um grupo de administração para cada distribuição Linux. Por exemplo, caso haja dispositivos Debian e Red Hat Linux, aloque-os em grupos de administração diferentes. Isso permitirá a execução da migração com êxito porque diferentes pacotes de instalação do Agente de Rede são necessários para vários sistemas operacionais.

2. **Realize separadamente a migração de cada grupo de administração e seus objetos de aplicação**

   Os dispositivos gerenciados de cada sistema operacional devem migrar separadamente para incluir suas políticas e tarefas. Por exemplo, caso haja dispositivos Windows, macOS, Ubuntu e CentOS, primeiramente transfira os dispositivos que executam o sistema operacional Windows para o Kaspersky Security Center Cloud Console; em seguida, macOS, Ubuntu e, por fim, CentOS. É possível transferir os dispositivos gerenciados em qualquer ordem.

   Para fazer isso, execute a migração sem a hierarquia de Servidores de Administração ou a migração com essa hierarquia, a depender se a rede inclui Servidores de Administração secundários. Durante a migração, utilize o pacote de instalação do Agente de Rede correspondente ao sistema operacional dos dispositivos transferidos. Por exemplo, selecione o Agente de Rede do Kaspersky Security Center 13.2 para dispositivos Linux para executar a migração com sucesso.

   Observe que os objetos não pertencentes a grupos, como as tarefas globais, as seleções de dispositivos personalizados ou os relatórios, precisam ser migrados apenas uma vez.

Resultados

Ao concluir a migração, você pode conferir se ela deu certo:

- A versão adequada do Agente de Rede é reinstalada em cada dispositivo gerenciado executando o sistema operacional Linux e/ou macOS.
- Todos os dispositivos Linux ou macOS são gerenciados pelo Kaspersky Security Center Cloud Console.
- Todas as configurações de objeto em vigor antes da migração serão preservadas.

Cenário: migração reversa do Kaspersky Security Center Cloud Console para o Kaspersky Security Center

Talvez seja boa ideia migrar os dispositivos gerenciados do Kaspersky Security Center Cloud Console para o Servidor de Administração do Kaspersky Security Center. Por exemplo, este processo pode ser usado para reverter a migração para o Kaspersky Security Center Cloud Console.

Pré-requisitos

Antes de iniciar, verifique se os seguintes pré-requisitos foram atendidos:

- O Kaspersky Security Center Cloud Console está disponível e tem dispositivos gerenciados conectados.
- O Servidor de Administração do Kaspersky Security Center 14.2 (ou posterior) está disponível e tem um pacote de instalação do Agente de Rede da versão 13 ou posterior.

Estágios de migração reversa

A migração reversa compreende os seguintes estágios:

1. **Criar um pacote de instalação independente do Agente de Rede no Servidor de Administração do Kaspersky Security Center local**

   No Servidor de Administração do Kaspersky Security Center executado no local, crie um pacote de instalação independente do Agente de Rede.

   Durante o processo de criação, é possível selecionar a opção **Migrar dispositivos não atribuídos para este grupo** para especificar um grupo de administração para o qual deseja mover Agentes de Rede após a instalação. Caso o grupo de administração tenha sido especificado, será criada uma regra de movimentação automática que moverá para o grupo de administração de destino todos os Agentes de Rede instalados com este pacote de instalação independente.

   > Para garantir a migração reversa adequada, certifique-se de selecionar a versão do Agente de Rede igual ou posterior à versão usada no Kaspersky Security Center Cloud Console.

2. **Criar um pacote de instalação personalizado no Kaspersky Security Center Cloud Console**

   No Kaspersky Security Center Cloud Console, crie um pacote de instalação personalizado com base no pacote de instalação independente criado e salvo do Servidor de Administração do Kaspersky Security Center executado localmente.

   Para ativar a instalação do pacote no modo silencioso, no campo **Linha de comando de arquivo executável**, especifique a chave `-s`.

3. **Criar uma tarefa de instalação remota**

   No Kaspersky Security Center Cloud Console, crie uma tarefa de instalação remota usando o pacote de instalação personalizado criado.

4. **Executar a tarefa de instalação remota**

   Inicie a tarefa de instalação remota que você criou. A tarefa inicia a reinstalação de todos os Agentes de Rede no grupo de administração especificado; além disso, ela troca os Agentes de Rede gerenciados no Servidor de Administração do Kaspersky Security Center em execução no local, alterando o endereço de conexão e modificando outras configurações de conexão.

   > Caso não tenha especificado nenhum grupo de administração de destino durante a criação do pacote de instalação independente, todos os dispositivos serão movidos para o grupo **Dispositivos não atribuídos**.

Resultados

Ao concluir a migração, você pode conferir se ela deu certo:

- Todos os dispositivos no escopo da tarefa de instalação remota gerenciados anteriormente pelo Kaspersky Security Center Cloud Console agora são gerenciados pelo Servidor de Administração do Kaspersky Security Center executado no local.
- Os dispositivos são movidos automaticamente para o grupo de administração especificado nas configurações do pacote de instalação.

A tarefa de instalação remota no Kaspersky Security Center Cloud Console não pôde ser concluída: ela não tem mais dispositivos de destino, pois todos tiveram suas configurações de conexão modificadas. Você deve interromper a tarefa manualmente depois de verificar se o ícone de erro (!) apareceu na coluna **Visível** da lista de dispositivos gerenciados para todos os dispositivos do escopo de migração.

Migração com Servidores de Administração virtuais

Se você possuir Servidores de Administração virtuais em sua infraestrutura local existente do Kaspersky Security Center, não poderá migrar do Kaspersky Security Center local para o Kaspersky Security Center Cloud Console usando o Assistente de Migração. Além disso, você poderá migrar apenas os dispositivos de seus clientes. Você terá que criar políticas, tarefas e relatórios manualmente.

É possível executar um dos seguintes cenários de migração:

- Mover os dispositivos clientes dos Servidores de Administração virtuais para um Servidor de Administração principal
- Executar a migração manual dos Servidores de Administração virtuais

Cenário: migração com Servidores de Administração virtuais movendo dispositivos

Para realizar a migração do Kaspersky Security Center Web Console executado localmente para o Kaspersky Security Center Cloud Console, é possível mover seus dispositivos de Servidores de Administração virtuais para um Servidor de Administração principal.

Pré-requisitos

Antes da migração, executar várias ações devem ser executadas, incluindo a atualização do Servidor de Administração em execução no local para a versão 12 ou posterior e a atualização dos aplicativos gerenciados para versões compatíveis com o Kaspersky Security Center Cloud Console.

Cenário de migração

O cenário continua em estágios:

1. **Criando um grupo de administração para cada um dos Servidores de Administração virtuais**

   Você pode criar o grupo no seu Kaspersky Security Center executado no local.

2. **Mover os dispositivos dos seus clientes**

No Kaspersky Security Center executado no local, mova os dispositivos de seus clientes de cada Servidor de Administração virtual para o respectivo grupo de administração criado no estágio anterior.

3. **Migração**

   Execute a migração conforme descrito para a rede sem hierarquia de Servidores de Administração.

4. **Migrando dispositivos sob gerenciamento de servidores de administração virtuais (etapa opcional)**

   Se você deseja gerenciar seus clientes por meio de servidores de administração virtuais, migre os dispositivos dos grupos de administração sob gerenciamento de Servidores de Administração virtuais.

5. **Criando políticas, tarefas e relatórios**

   Criar políticas, tarefas e relatórios, conforme necessário.

Resultados

Ao concluir a migração, você pode conferir se ela deu certo:

- O Agente de Rede é reinstalado em todos os dispositivos gerenciados.
- Todos os dispositivos são gerenciados pelo Kaspersky Security Center Cloud Console.
- Todas as configurações de objeto em vigor antes da migração serão preservadas.

Cenário: migração manual com Servidores de Administração virtuais

Você pode migrar manualmente do Kaspersky Security Center Web Console executado no local para o Kaspersky Security Center Cloud Console.

Pré-requisitos

Antes da migração, executar várias ações devem ser executadas, incluindo a atualização do Servidor de Administração em execução no local para a versão 12 ou posterior e a atualização dos aplicativos gerenciados para versões compatíveis com o Kaspersky Security Center Cloud Console.

Cenário de migração

O cenário continua em estágios:

1. **Criando um grupo de administração para cada um dos Servidores de Administração virtuais**

   No Kaspersky Security Center Cloud Console, criar um grupo de administração que corresponda a cada um dos seus Servidores de Administração virtuais.

2. **Criar um pacote de instalação independente para o Agente de Rede**

   Criando um pacote de instalação independente para o Agente de Rede. Durante a criação, especifique o grupo de administração que você criou no estágio anterior. Isso significa que você deve criar um pacote de instalação independente individual para cada grupo de administração.

   Este estágio ocorre no Kaspersky Security Center Cloud Console.

3. **Baixando os pacotes de instalação independente**

   Fazer o download dos pacotes de instalação independentes criados no estágio anterior. Este estágio ocorre no Kaspersky Security Center Cloud Console.

4. **Criar um arquivo compactado com cada pacote de instalação independente**

   Os tipos de arquivos compactados disponíveis são: ZIP, CAB, TAR ou TAR.GZ.

5. **Criando pacotes de instalação personalizados para o Agente de Rede**

   Criar pacotes de instalação independente para o Agente de Rede. Durante a criação, use os arquivos compactados que você criou no estágio anterior.

   Este estágio ocorre no seu Kaspersky Security Center executado no local.

6. **Criando tarefas de instalação remota**

   Criar tarefas de instalação remota para instalar o Agente de Rede a partir dos pacotes de instalação personalizados criados.

   Ao criar uma tarefa, especifique um grupo de administração correspondente.

   Este estágio ocorre no seu Kaspersky Security Center executado no local.

7. **Executar as tarefas de instalação remota criadas**

   Os Agentes de Rede são atualizados. O Servidor de Administração do Kaspersky Security Center Cloud Console assume o gerenciamento deles.

   Todos os dispositivos são migrados para o Kaspersky Security Center Cloud Console e são colocados nos grupos de administração especificados ao criar os pacotes de instalação independentes para o Agente de Rede.

8. **Migrando dispositivos sob gerenciamento de servidores de administração virtuais (etapa opcional)**

   Se você deseja gerenciar seus clientes por meio de servidores de administração virtuais, migre os dispositivos dos grupos de administração sob gerenciamento de Servidores de Administração virtuais.

9. **Criando políticas, tarefas e relatórios**

   Criar políticas, tarefas e relatórios, conforme necessário.

Resultados

Ao concluir a migração, você pode conferir se ela deu certo:

- O Agente de Rede é reinstalado em todos os dispositivos gerenciados.
- Todos os dispositivos são gerenciados pelo Kaspersky Security Center Cloud Console.

  Todas as configurações de objeto em vigor antes da migração serão preservadas.

Cenário: mover dispositivos de grupos de administração sob gerenciamento de servidores virtuais

Você pode desejar gerenciar seus clientes por meio de Servidores de Administração virtuais. Se você migrou dispositivos e outros itens do Kaspersky Security Center local para o Kaspersky Security Center Cloud Console, os dispositivos estão localizados em grupos de administração. Para gerenciar os dispositivos dos clientes por meio de Servidores de Administração virtuais, você deve migrar os dispositivos dos grupos de administração sob o gerenciamento de Servidores de Administração virtuais.

Pré-requisitos

Você criou um servidor de administração virtual para cada um de seus clientes.

Todos os dispositivos de cada cliente estão localizados em um grupo de administração individual.

Fases

O cenário continua em estágios:

1. **Criar um pacote de instalação independente para o Agente de Rede**

   Migre para cada um dos Servidores de Administração virtuais criados. Depois, crie um pacote de instalação independente para o Agente de Rede. Você pode alternar os Servidores de Administração no menu principal, clicando no ícone de seta dupla () à direita do nome do Servidor de Administração atual. Depois, selecione o Servidor de Administração necessário.

2. **Baixando os pacotes de instalação independente**

   Fazer o download dos pacotes de instalação independentes criados no estágio anterior.

3. **Crie um arquivo compactado com cada pacote de instalação independente**

   Os tipos de arquivos compactados disponíveis são: ZIP, CAB, TAR ou TAR.GZ.

4. **Criando pacotes de instalação personalizados para o Agente de Rede**

   Criar pacotes de instalação independente para o Agente de Rede. Durante a criação, use os arquivos compactados que você criou no estágio anterior.

   Esta fase ocorre no Servidor de Administração principal.

5. **Criando tarefas de instalação remota**

   Criar tarefas de instalação remota para instalar o Agente de Rede a partir dos pacotes de instalação personalizados criados.

   Ao criar uma tarefa, especifique um grupo de administração correspondente.

   Esta fase ocorre no Servidor de Administração principal.

6. **Execute as tarefas de instalação remota criadas**

   Os Agentes de Rede são atualizados. Os dispositivos são migrados sob gerenciamento de Servidores de Administração virtuais.

7. **Criando políticas, tarefas e relatórios**

   Criar políticas, tarefas e relatórios, conforme necessário.

Resultados

Agora você pode gerenciar os dispositivos migrados dos clientes usando Servidores de Administração virtuais.

Assistente de início rápido

Esta seção fornece informações sobre o Assistente de Início Rápido do Kaspersky Security Center Cloud Console.

Sobre o Assistente de Início Rápido

O Assistente de Início Rápido no Kaspersky Security Center Cloud Console permite criar um conjunto mínimo de tarefas e políticas necessárias, ajustar uma configuração mínima e iniciar a criação de pacotes de instalação de aplicativos Kaspersky. Usando o assistente, é possível fazer as seguintes alterações no Kaspersky Security Center Cloud Console:

- Inicie o download de pacotes de instalação para aplicativos gerenciados da Kaspersky.
- Crie um pacote de instalação independente do Agente de Rede para dispositivos que executam Windows, Linux ou macOS.
- Criar politica do Agente de Rede do Kaspersky Security Center.
- Criar a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*.
- Criar políticas e tarefas para aplicativos gerenciados da Kaspersky.
- Configure a interação com a Kaspersky Security Network (KSN).

Após a conclusão do Assistente de início rápido, os pacotes de instalação do Agente de Rede e dos aplicativos Kaspersky gerenciados aparecem na lista **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**.

O Assistente de Início Rápido cria políticas para aplicativos gerenciados, como o Kaspersky Endpoint Security for Windows, a menos que tais políticas sejam criadas para o grupo de Dispositivos gerenciados. O Assistente de Início Rápido cria tarefas se tarefas com o mesmo nome não existirem para o grupo de Dispositivos gerenciados.

O Kaspersky Security Center Cloud Console solicita automaticamente a execução do Assistente de início rápido após você ter criado um espaço de trabalho da empresa e iniciado o Kaspersky Security Center Cloud Console pela primeira vez. Você também pode iniciar o Assistente de início rápido manualmente a qualquer momento.

Iniciar Assistente de início rápido

O Kaspersky Security Center Cloud Console solicita automaticamente a execução do Assistente de início rápido após você ter criado um espaço de trabalho da empresa e iniciado o Kaspersky Security Center Cloud Console pela primeira vez. Você também pode iniciar o Assistente de início rápido manualmente a qualquer momento.

Caso o Assistente de Início Rápido seja iniciado novamente, as tarefas e políticas criadas na execução anterior do Assistente não serão recriadas.

Para iniciar o Assistente de Início Rápido manualmente:

1. No menu principal, clique no ícone de configurações () ao lado do nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Geral**.

3. Clique em **Iniciar o assistente de início rápido**.

   Como alternativa, é possível iniciar o Assistente de início rápido selecionando **Descoberta e implementação → Implementação e atribuição → Assistente de início rápido**.

O assistente solicita que você execute a configuração inicial do Kaspersky Security Center Cloud Console. Siga as instruções do Assistente. Prossiga pelo assistente usando o botão **Avançar**. Use o botão **Voltar** para retornar para a etapa anterior do assistente.

Etapa 1. Seleção de pacotes de instalação para download

Na lista, selecione os aplicativos Kaspersky para instalar nos dispositivos clientes. O Kaspersky Security Center Cloud Console criará pacotes de instalação para os aplicativos selecionados. Em seguida, você usará os pacotes de instalação criados para instalar os aplicativos.

Ao selecionar um pacote de instalação para baixar, atente para o idioma: os pacotes de instalação estão disponíveis em diferentes idiomas.

Selecione os seguintes aplicativos:

- Agente de Rede do Kaspersky Security Center

  Ao selecionar pacotes de instalação do Agente de Rede, considere o seguinte:

  - O Agente de Rede deve ser instalado em cada dispositivo cliente. Portanto, selecione um Agente de Rede apropriado para cada sistema operacional executado nos dispositivos clientes.

  - O Agente de Rede deve ser instalado manualmente por meio de um pacote de instalação independente em um dispositivo que você seleciona para atuar como ponto de distribuição. Os pontos de distribuição são necessários para executar amostragem de rede e a instalação remota dos aplicativos de segurança Kaspersky nos dispositivos clientes. Portanto, você deve selecionar pelo menos um pacote de instalação do Agente de Rede. Enquanto você prossegue para as próximas etapas do assistente, o Kaspersky Security Center Cloud Console cria o pacote de instalação independente do Agente de Rede.

    Comparado aos pontos de distribuição baseados no Windows, os pontos de distribuição baseados no Linux e no macOS têm funcionalidade limitada. É altamente recomendável que você selecione computadores baseados no Windows para atuarem como pontos de distribuição.

    Você pode selecionar Agentes de Rede para Windows, Linux e macOS. Se você selecionar o Agente de Rede apenas para um sistema operacional, por exemplo, macOS, um pacote de instalação independente será criado para o sistema operacional selecionado. Se você selecionar o Agente de Rede para vários sistemas operacionais, o Kaspersky Security Center Cloud Console criará apenas um pacote de instalação independente de acordo com as seguintes prioridades: o Windows é da mais alta prioridade, seguido pelo Linux e o macOS. Por exemplo, se você selecionar Agentes de Rede para Linux e macOS, o Kaspersky Security Center Cloud Console criará um pacote de instalação independente para o Agente de Rede para Linux. Você pode criar um pacote de instalação independente do Agente de Rede para qualquer um desses sistemas operacionais manualmente a qualquer momento.

- Aplicativos de segurança Kaspersky

  Selecione os pacotes de instalação apropriados para os sistemas operacionais instalados nos dispositivos clientes da sua organização.

Etapa 2. Configurar um servidor proxy

Se sua organização usa um servidor proxy para se conectar à Internet, especifique as configurações do servidor proxy nesta etapa do assistente. Estas configurações são adicionadas ao pacote de instalação do Agente de Rede. Após a instalação, o Agente de Rede usa essas configurações automaticamente em cada dispositivo cliente.

Especifique as seguintes configurações para a conexão ao servidor proxy:

- **Usar o servidor proxy**
- **Endereço**
- **Número da porta**
- Autenticação do servidor proxy

  Se esta caixa de seleção estiver marcada, você poderá especificar as credenciais para a autenticação do servidor proxy.

  Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

  Por padrão, esta opção está desativada.

- Nome do usuário

  Nome do usuário sob o qual a conexão ao servidor proxy é estabelecida.

  Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

- Senha

  Nome do usuário sob a qual a conexão ao servidor proxy é estabelecida.

  Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

Etapa 3. Configurar a Kaspersky Security Network

Se, na etapa anterior do assistente, você baixou o pacote de instalação do Kaspersky Endpoint Security for Windows, o texto da Declaração KSN para os seguintes aplicativos será exibido:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security Center instalado em dispositivos locais
- Kaspersky Security Center Cloud Console instalado no ambiente em nuvem

Se você não baixou o pacote de instalação do Kaspersky Endpoint Security for Windows, a Declaração KSN para este aplicativo não será exibida.

No modo de avaliação, apenas a Declaração KSN do Kaspersky Endpoint Security for Windows é exibida.

Leia com atenção a Declaração da Kaspersky Security Network. Selecione uma das seguintes opções:

- **Concordo em usar a Kaspersky Security Network**

  O Kaspersky Security Center Cloud Console e os aplicativos gerenciados instalados nos dispositivos cliente transferem automaticamente seus detalhes de operação para a Kaspersky Security Network. A participação na Kaspersky Security Network assegura atualizações mais rápidas dos bancos de dados que contêm informações sobre vírus e outras ameaças, que assegura uma resposta mais rápida a ameaças de segurança emergentes.

- **Não concordo em usar a Kaspersky Security Network**

  O Kaspersky Security Center Cloud Console e os aplicativos gerenciados não fornecerão informações à Kaspersky Security Network.

  Se você selecionar esta opção, o uso da Kaspersky Security Network será desativado.

Por padrão, o uso da KSN está desativado. Posteriormente, se você mudar de ideia sobre o uso da KSN, poderá ativar (ou desativar) a opção correspondente na janela de propriedades do Servidor de Administração, na seção **Configurações da KSN**.

Etapa 4. Configuração do gerenciamento de atualizações de terceiros

Essa etapa não é exibida se a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* já existir.

Caso deseje obter uma lista de atualizações para os aplicativos instalados nos dispositivos gerenciados e uma lista de vulnerabilidades encontradas e correções recomendadas, habilite a opção **Pesquisar por atualizações e correções de vulnerabilidades de softwares de terceiros**. Se essa opção for ativada, o Kaspersky Security Center Cloud Console cria a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

Etapa 5. Criar uma configuração básica de proteção de rede

Nesta etapa do assistente, clique no ícone **Criar** para criar objetos necessários para a proteção inicial dos seus dispositivos clientes.

O Kaspersky Security Center Cloud Console executa duas operações:

- Criar políticas e tarefas básicas com configurações padrão

  As seguintes políticas são criadas:

  - Política do Agente de Rede do Kaspersky Security Center
  - Políticas para aplicativos gerenciados da Kaspersky

  As seguintes tarefas são criadas:

  - A tarefa *Baixar atualizações para os repositórios de pontos de distribuição*

- A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*

  A tarefa só é criada caso a opção **Pesquisar por atualizações e correções de vulnerabilidades de softwares de terceiros** tenha sido ativada na etapa anterior do assistente.

- Tarefas para aplicativos gerenciados Kaspersky

- Criar um pacote de instalação independente para o Agente de Rede

  Você usará este pacote para instalar o Agente de Rede nos pontos de distribuição. O Kaspersky Security Center Cloud Console cria o pacote de instalação independente com base no pacote de instalação do Agente de Rede selecionado na etapa anterior do assistente. Durante a criação do pacote, você deve ler e aceitar os termos do EULA para o Agente de Rede. Quando o pacote de instalação independente for criado, será solicitado que você faça o download dele no dispositivo usado no momento.

  A criação do pacote de instalação independente do Agente de Rede pode levar algum tempo. É possível prosseguir para a próxima etapa do assistente. O processo continuará no modo de segundo plano. É possível acompanhar o processo na guia **Em andamento ()** da seção **Pacotes de instalação** (**Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**).

  Por motivos de autenticação, cada pacote de instalação independente é assinado usando um certificado. O certificado é reemitido periodicamente. Após cada procedimento de reemissão do certificado, o Kaspersky Security Center Cloud Console atualiza automaticamente as assinaturas de todos os pacotes de instalação independentes criados. Para pacotes de instalação independentes baixados, uma atualização automática de assinaturas não pode ser executada. Portanto, o certificado expira e pode ocorrer um erro de certificado enquanto você instala um aplicativo a partir de um pacote de instalação independente. Nesse caso, baixe o pacote de instalação independente novamente.

Etapa 6. Fechar o Assistente de início rápido

Na página de conclusão do Assistente de Início Rápido, leia sobre as operações adicionais que devem ser executadas para implantar aplicativos de segurança Kaspersky nos dispositivos clientes. Siga os estágios fornecidos no cenário de implementação inicial dos aplicativos Kaspersky.

Implementação inicial dos aplicativos da Kaspersky

Esta seção descreve a implementação inicial dos aplicativos Kaspersky nos dispositivos cliente da sua organização.

Cenário: Verificando a implementação inicial dos aplicativos Kaspersky

Este cenário descreve como instalar aplicativos Kaspersky em dispositivos cliente no Kaspersky Security Center Cloud Console. Primeiro, você deve implementar pontos de distribuição na sua rede. Em seguida, por meio dos pontos de distribuição, você deve executar uma sondagem da rede e localizar dispositivos em rede na sua rede. Após disso, você pode implementar aplicativos da Kaspersky nos dispositivos em rede.

Quando o cenário for concluído, os aplicativos Kaspersky serão implementados nos dispositivos cliente selecionados na rede da sua organização. Você pode gerenciar todos os dispositivos com os aplicativos Kaspersky instalados.

Pré-requisitos

Antes de iniciar, verifique se os seguintes pré-requisitos foram atendidos:

- O Assistente de Início Rápido foi concluído.
- Os pacotes de instalação do Agente de Rede e dos aplicativos de segurança são criados.
- O endereço https://aes.s.kaspersky-labs.com/endpoints/ está incluído nas exceções do Firewall do dispositivo gerenciado.
- Você tem informações sobre configurações de Internet para dispositivos cliente na sua organização, informações sobre configurações do gateway e servidor proxy.

Fases

A implementação inicial dos aplicativos Kaspersky prossegue em fases:

1. **Selecionando um dispositivo para agir como ponto de distribuição**

   No Kaspersky Security Center Cloud Console, um ponto de distribuição é destinado a:

   - Sondagem da rede e descoberta de dispositivos
   - Instalação remota do Agente de Rede em dispositivos cliente
   - Conexão de dispositivos cliente com o Servidor de Administração (quando um ponto de distribuição está atuando como gateway de conexão)

   Selecione um dispositivo na rede da sua organização para atuar como um ponto de distribuição para um grupo de administração. O dispositivo selecionado deve atender aos requisitos de ponto de distribuição. Dependendo da quantidade de dispositivos cliente na rede da sua organização, selecione o número correto de dispositivos para atuar como pontos de distribuição.

2. **Criar um pacote de instalação independente para o Agente de Rede**

   Crie um pacote de instalação independente para o Agente de Rede instalá-lo no ponto de distribuição.

Se seus dispositivos clientes não tiverem acesso à Internet para se conectarem diretamente com o Servidor de Administração, nas configurações do pacote de instalação do Agente de Rede, defina as configurações do gateway de conexão e do servidor proxy.

3. **Instalar o Agente de Rede no dispositivo selecionado para atuar como um ponto de distribuição**

   Entregue o pacote de instalação independente do Agente de Rede ao dispositivo selecionado por qualquer método. Por exemplo, você pode copiar o pacote de instalação independente para uma unidade removível (como um pen drive) ou colocá-lo em uma pasta compartilhada.

   Na janela **Propriedades** do arquivo do pacote de instalação independente, verifique se o pacote de instalação independente do Agente de Rede está assinado pela Kaspersky.

   Execute a instalação do pacote de instalação independente do Agente de Rede no dispositivo selecionado. Agora o Agente de Rede é instalado de acordo com as configurações do pacote de instalação do Agente de Rede e conectado ao Servidor de Administração. O dispositivo com o Agente de Rede é colocado no grupo de administração especificado quando o pacote de instalação independente para o Agente de Rede foi criado.

   Se você instalar o Agente de Rede usando um pacote de instalação independente em um dispositivo executando o Microsoft Windows XP Professional for Embedded Systems 32 bits, a instalação falhará. Para resolver esse problema, instale primeiro a atualização KB2868626 para o Windows XP no site da Microsoft: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

4. **Atribuir o dispositivo com o Agente de Rede instalado para atuar como um ponto de distribuição**

   Atribuir o dispositivo com o Agente de Rede instalado para atuar como um ponto de distribuição.

5. **Configurando e executando uma sondagem de rede para o ponto de distribuição**

   Configure a sondagem de rede para o ponto de distribuição com o Agente de Rede instalado. Como alternativa, você pode configurar a sondagem da rede na política do Agente de Rede.

   Após a conclusão da sondagem da rede conforme o agendamento, os dispositivos cliente conectados à rede da sua organização são localizados e colocados no grupo **Dispositivos não atribuídos**.

6. **Criando pacotes de instalação para o Agente de Rede e os aplicativos gerenciados Kaspersky**

   Caso não tenha iniciado o Assistente de Início Rápido ou tenha ignorado a etapa de criação de pacotes de instalação, crie pacotes de instalação para os aplicativos Kaspersky. É necessário criar pacotes de instalação tanto para o agente de rede quanto para os aplicativos gerenciados Kaspersky apropriados para o sistema operacional instalado nos dispositivos cliente na rede da sua organização.

7. **Removendo aplicativos de segurança de terceiros**

   Se aplicativos de segurança de terceiros estiverem instalados nos dispositivos clientes da rede da sua organização, remova-os antes de instalar os aplicativos Kaspersky.

8. **Instalando aplicativos Kaspersky em dispositivos cliente**

   Crie tarefas para instalar o Agente de Rede e os aplicativos gerenciados da Kaspersky em dispositivos cliente na rede da sua organização. Ao criar as tarefas, use o tipo de tarefa **Instalar o aplicativo remotamente**. Para a tarefa de instalar o Agente de Rede, use a opção **Usando recursos do sistema operacional através de pontos de distribuição**. Para a tarefa de instalar aplicativos gerenciados da Kaspersky, use a opção **Usando o Agente de Rede**. Após a criação das tarefas, você pode definir as suas configurações. Certifique-se de que o agendamento de cada tarefa atenda aos seus requisitos. Primeiro, a tarefa para instalar o Agente de Rede deve ser executada. Em seguida, após a instalação do Agente de Rede nos dispositivos cliente, a tarefa para instalar os aplicativos gerenciados da Kaspersky deve ser executada.

   Como opção, é possível criar uma tarefa de instalação remota para instalar o Agente de Rede e os aplicativos gerenciados da Kaspersky em dispositivos cliente na rede da sua organização. Nesse caso, no bloco **Pacotes de instalação**, use a opção **Selecionar o pacote de instalação** e a opção **Selecionar Agente de Rede**; no bloco **Forçar download do pacote de instalação**, use a opção **Usando recursos do sistema operacional através de pontos de distribuição**.

Você também pode criar várias tarefas de instalação remota para instalar aplicativos gerenciados da Kaspersky para diferentes grupos de administração ou seleções de dispositivos diferentes.

Se você tiver dispositivos cliente que estão fora da rede com ponto de distribuição, por exemplo, laptops de usuários remotos, deverá criar e entregar o pacote de instalação independente do Agente de Rede a esses dispositivos cliente por qualquer método. Instale o pacote de instalação independente do Agente de Rede localmente nesses dispositivos cliente. Em seguida, você pode instalar os aplicativos gerenciados da Kaspersky nos dispositivos desses usuários remotos, seguindo as mesmas instruções para os outros dispositivos descobertos pelo ponto de distribuição.

Executar as tarefas de instalação remota.

Como opção, para a instalação de aplicativos Kaspersky, é possível iniciar o Assistente de Implementação de Proteção.

9. **Instalando o Kaspersky Security for Mobile**

   Se você planeja gerenciar dispositivos móveis corporativos, siga as instruções fornecidas no Ajuda do Kaspersky Security for Mobile para obter informações sobre a implementação do Kaspersky Endpoint Security for Android.

10. **Verificando a implementação inicial dos aplicativos Kaspersky**

    Gere e visualize o **Relatório de versões de software da Kaspersky**. Verifique se os aplicativos Kaspersky gerenciados estão instalados em todos os dispositivos cliente na sua organização.

Para a criptografia completa do disco, o Kaspersky Security Center Cloud Console é compatível apenas com o BitLocker.

Criar pacotes de instalação para aplicativos da Kaspersky

Para implementar aplicativos Kaspersky em dispositivos de rede da sua organização, você deve criar pacotes de instalação dos aplicativos Kaspersky no Kaspersky Security Center Cloud Console.

Para criar um pacote de instalação do aplicativo Kaspersky:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**.
   - No menu principal, vá para **Operações → Repositórios → Pacotes de instalação**.

   Também é possível visualizar as notificações sobre novos pacotes na lista de notificações na tela. Se houver notificações sobre um novo pacote, você poderá clicar no link ao lado da notificação e prosseguir para a lista de pacotes de instalação disponíveis.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Clique em **Adicionar**.

   O assistente de Nova categoria inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na primeira página do assistente, selecione **Criar um pacote de instalação para um aplicativo da Kaspersky**.

   Uma lista dos pacotes de distribuição disponíveis nos servidores da Web Kaspersky é exibida.

4. Clique no nome de um pacote de instalação, por exemplo, **Kaspersky Endpoint Security for Windows (<número da versão>)**.

   Uma janela é exibida com informações sobre o pacote de distribuição.

5. Leia as informações e clique no botão **Baixar e criar o pacote de instalação**.

   Se um pacote de distribuição não puder ser convertido automaticamente em um pacote de instalação, o botão **Baixar o pacote de distribuição** será exibido em vez do botão **Baixar e criar o pacote de instalação**. Nesse caso, baixe o pacote de distribuição e use o arquivo baixado para criar um pacote de instalação personalizado.

   O download do pacote de instalação é iniciado. É possível fechar a janela do assistente ou prosseguir para a próxima etapa da instrução. Caso a janela do assistente seja fechada, o processo de download continuará no modo de segundo plano.

   Se você deseja acompanhar um processo de download do pacote de instalação:

   a. No menu principal, vá para **Operações** → **Repositórios** → **Pacotes de instalação** → **Em andamento ()**.

   b. Acompanhe o progresso da operação na coluna **Progresso do download** e na coluna **Status do download** da tabela.

   Quando o processo for concluído, o pacote de instalação será adicionado à lista na guia **Baixado**. Se o processo de download for interrompido e o status do download mudar para **Aceitar EULA**, clique no nome do pacote de instalação e prossiga para a próxima etapa da instrução.

   Se você planeja realizar a migração do Kaspersky Security Center Web Console para o Kaspersky Security Center Cloud Console e os regulamentos de segurança da sua organização exigem o uso de proxy para acessar a rede corporativa, isso pode afetar o processo de migração. Depois de criar um pacote de instalação do Agente de Rede, você deve especificar as configurações de proxy para garantir a conexão entre as instâncias do Agente de Rede em dispositivos gerenciados e seu espaço de trabalho do Kaspersky Security Center Cloud Console:

   a. Clique no nome do pacote de instalação.

   b. Na janela de propriedades do pacote de instalação exibida, acesse a guia **Configurações**.

   c. Abra a seção **Conexão**.

   d. Selecione a opção **Usar o servidor proxy** e preencha os campos **Endereço do servidor proxy** e **Porta do servidor proxy**.

6. Para alguns aplicativos da Kaspersky, o botão **Mostrar EULA** será exibido durante o processo de download. Se ele for exibido, faça o seguinte:

   a. Clique no botão **Mostrar EULA** para ler o Contrato de Licença do Usuário Final (EULA).

   b. Leia o EULA, que é exibido na tela, e clique no botão **Aceitar**.

      O download continua depois que você aceita o EULA. Se clicar em **Recusar**, o download será interrompido.

7. Quando o download estiver concluído, clique no botão **Fechar** (×) para fechar a janela com informações sobre o pacote de distribuição.

O pacote de instalação é criado. O pacote de instalação aparece na lista de pacotes de instalação.

Distribuindo pacotes de instalação para Servidores de Administração secundários

Para distribuir pacotes de instalação para Servidores de Administração secundários:

1. Estabeleça uma conexão ao Servidor de Administração que controla os Servidores de Administração secundários relevantes.

2. Crie uma tarefa de distribuição de pacotes de distribuição para Servidores de Administração secundários de uma das seguintes formas:

   - Se desejar criar uma tarefa para Servidores de Administração secundários no grupo de administração selecionado, inicie a criação de uma tarefa de grupo para esse grupo.

   - Caso deseje criar uma tarefa para Servidores de Administração secundários específicos, inicie a criação de uma tarefa para dispositivos específicos.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

   Na janela **Nova tarefa** do Assistente para novas tarefas, no campo **Tipo de tarefa**, selecione **Distribuir pacote de instalação**. Você também pode editar o nome padrão da tarefa no campo **Nome da tarefa**.

   No próximo passo, especifique os Servidores de Administração secundários para o escopo da tarefa e siga as instruções do assistente para Adicionar tarefas. Ao terminar, o assistente para adicionar tarefas criará a tarefa de distribuição dos pacotes de instalação selecionados nos Servidores de Administração secundários específicos.

   Ao criar a tarefa Distribuir o pacote de instalação para Servidores de Administração secundários executados no local, o escopo de distribuição, além de pacotes de instalação personalizados, incluirá apenas os pacotes de instalação dos aplicativos Kaspersky compatíveis com o Kaspersky Security Center Web Console executado no local, independentemente da opção de distribuição selecionada (**Todos os pacotes de instalação** ou **Pacotes de instalação selecionados**).

3. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação que você especificou nas configurações da tarefa.

Os pacotes de instalação selecionados serão copiados para os Servidores de Administração secundários específicos.

Criar pacotes de instalação independentes para o Agente de Rede

Você e os usuários de dispositivos na sua organização podem usar pacotes de instalação independente para instalar o Agente de Rede em dispositivos localmente. Pacotes de instalação independentes podem ser criados para dispositivos executando Windows, Linux ou macOS.

No Kaspersky Security Center Cloud Console, você pode criar pacotes de instalação independentes apenas para o Agente de Rede.

Um pacote de instalação independente é um arquivo executável que pode ser enviado por e-mail ou transferido para um dispositivo cliente por outro método. O arquivo recebido pode ser executado localmente no dispositivo cliente para instalar o Agente de Rede sem envolver o Kaspersky Security Center Cloud Console.

Para o Agente de Rede para o Linux e para o Agente de Rede para o macOS, o pacote de instalação independente é um arquivo de script com a extensão .sh. Quando você executa este arquivo, o script descompacta o arquivo anexado que contém o pacote de instalação e suas configurações e, a seguir, inicia a instalação.

Se você instalar o Agente de Rede usando um pacote de instalação independente em um dispositivo executando o Microsoft Windows XP Professional for Embedded Systems 32 bits, a instalação falhará. Para resolver esse problema, instale primeiro a atualização KB2868626 para o Windows XP no site da Microsoft: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

Por motivos de autenticação, cada pacote de instalação independente é assinado usando um certificado. O certificado é reemitido periodicamente. Após cada procedimento de reemissão do certificado, o Kaspersky Security Center Cloud Console atualiza automaticamente as assinaturas de todos os pacotes de instalação independentes criados. Para pacotes de instalação independentes baixados, uma atualização automática de assinaturas não pode ser executada. Portanto, o certificado expira e pode ocorrer um erro de certificado enquanto você instala um aplicativo a partir de um pacote de instalação independente. Nesse caso, baixe o pacote de instalação independente novamente.

Para criar um pacote de instalação independente:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**.
   - No menu principal, vá para **Operações → Repositórios → Pacotes de instalação**.

   Uma lista de pacotes de instalação é exibida. Se o pacote de instalação do Agente de Rede não estiver na lista, crie esse pacote de instalação manualmente.

2. Na lista de pacotes de instalação, clique no nome do pacote de instalação do Agente de Rede.

   A janela de propriedades do pacote de instalação do Agente de Rede é exibida.

3. Defina as configurações do pacote de instalação do Agente de Rede, se necessário, e feche a janela de propriedades do pacote de instalação do Agente de Rede.

4. Na lista de pacotes de instalação, selecione um pacote de instalação e, acima da lista, clique no botão **Implementar**.

5. Selecione a opção **Usando um pacote autônomo**.

   O Assistente de Criação de Pacote de Instalação Independente é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

6. Na primeira página do assistente, verifique e confirme se a opção **Instalar o Agente de Rede junto com este aplicativo** está ativada, caso deseje instalar o Agente de Rede juntamente com o aplicativo selecionado.

   Por padrão, esta opção está ativada. É recomendável ativar esta opção se não tiver certeza se o Agente de Rede está instalado no dispositivo. Se o Agente de Rede já estiver instalado no dispositivo, após a instalação do pacote de instalação independente com o Agente de Rede, esse será atualizado para a versão mais recente.

   Se você desativar esta opção, o Agente de Rede não será instalado no dispositivo e esse não será gerenciado.

   Se já existir um pacote de instalação independente para o aplicativo selecionado no Servidor de Administração, o assistente informará a respeito. Nesse caso, você deve selecionar uma das seguintes ações:

   - **Criar pacote de instalação independente**. Selecione esta opção, por exemplo, se deseja criar um pacote de instalação independente para uma nova versão do aplicativo e também deseja manter um pacote de instalação independente criado para uma versão anterior do aplicativo. O novo pacote de instalação independente é colocado em outra pasta.
   - **Usar pacote de instalação independente existente**. Selecione esta opção se desejar usar um pacote de instalação independente existente. O processo de criação do pacote não será iniciado.

- **Recriar pacote de instalação independente existente**. Selecione esta opção se desejar criar um pacote de instalação independente para o mesmo aplicativo novamente. O pacote de instalação independente é colocado na mesma pasta.

7. Na página **Migrar para a lista de dispositivos gerenciados** do assistente, a opção **Não migrar dispositivos** é selecionada por padrão. Se você não deseja mover o dispositivo cliente para nenhum grupo de administração após a instalação do Agente de Rede, não modifique a opção.

   Se quiser mover os dispositivos clientes após a instalação do Agente de Rede, selecione a opção **Migrar dispositivos não atribuídos para este grupo** e especifique um grupo de administração para o qual você deseja mover o dispositivo cliente. Por padrão, o dispositivo é movido para o grupo **Dispositivos gerenciados**.

8. Na próxima página do assistente, selecione a opção **Abrir a lista de pacotes independentes** caso queira que a lista de pacotes de instalação independentes seja exibida após a conclusão do assistente.

9. Clique no botão **Concluir**.

   O Assistente de Criação de Pacote de Instalação Independente é fechado.

O pacote de instalação independente do Agente de Rede é criado. O pacote de instalação independente criado é exibido na lista de pacotes de instalação independente que você pode visualizar.

Visualizar a lista de pacotes de instalação independente

Você pode visualizar a lista de pacotes de instalação independente e as propriedades de cada pacote de instalação independente.

Para visualizar a lista de pacotes de instalação independente para todos os pacotes de instalação:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**.
   - No menu principal, vá para **Operações → Repositórios → Pacotes de instalação**.

   Uma lista de pacotes de instalação é exibida.

2. Acima da lista, clique no botão **Exibir a lista de pacotes independentes**.

Uma lista de pacotes de instalação independente exibida.

Na lista de pacotes de instalação independentes, suas propriedades são exibidas da seguinte maneira:

- **Nome do pacote**. Nome do pacote de instalação independente que é formado automaticamente como o nome do aplicativo incluído no pacote e na versão do aplicativo.
- **Nome do pacote de instalação do Agente de Rede**.
- **Versão do Agente de Rede**.
- **Tamanho**. Tamanho do arquivo em (MB).
- **Grupo**. Nome do grupo para o qual o dispositivo cliente é movido após a instalação do Agente de Rede.

- **Criação**. Data e hora da criação do pacote de instalação independente.
- **Modificação**. Data e hora da modificação do pacote de instalação independente.
- **Hash do arquivo**. A propriedade é usada para certificar que o pacote de instalação independente não foi alterado por terceiros e que um usuário tem o mesmo arquivo que você criou e transferiu para o usuário.

Para visualizar a lista de pacotes de instalação independente para um pacote de instalação específico:

Selecione o pacote de instalação na lista e, acima da lista, clique no botão **Exibir a lista de pacotes independentes**.

Na lista de pacotes de instalação independentes, você pode fazer o seguinte:

- Baixe um pacote de instalação independente para o seu dispositivo clicando no botão **Baixar**.

  Por motivos de autenticação, cada pacote de instalação independente é assinado usando um certificado. O certificado é reemitido periodicamente. Após cada procedimento de reemissão do certificado, o Kaspersky Security Center Cloud Console atualiza automaticamente as assinaturas de todos os pacotes de instalação independentes criados. Para pacotes de instalação independentes baixados, uma atualização automática de assinaturas não pode ser executada. Portanto, o certificado expira e pode ocorrer um erro de certificado enquanto você instala um aplicativo a partir de um pacote de instalação independente. Nesse caso, baixe o pacote de instalação independente novamente.

- Remova um pacote de instalação independente clicando no botão **Remover**.

Criar pacotes de instalação personalizados

Você pode usar pacotes de instalação personalizados para o seguinte:

- Para instalar qualquer aplicativo (por exemplo, um editor de texto) em um dispositivo cliente que envolva o Kaspersky Security Center Cloud Console, por exemplo, por meio de uma tarefa.
- Para criar um pacote de instalação independente.

Um pacote de instalação personalizado é uma pasta com um conjunto de arquivos, incluindo um arquivo executável. Uma fonte para criar um pacote de instalação personalizado é um arquivo morto. O arquivo morto contém um arquivo ou arquivos que precisam ser incluídos no pacote de instalação personalizado. Ao criar um pacote de instalação personalizado, é possível especificar as opções da linha de comando, por exemplo, para instalar o aplicativo em um modo silencioso.

Para criar um pacote de instalação personalizado:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**.
   - No menu principal, vá para **Operações → Repositórios → Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Clique em **Adicionar**.

   O assistente de Nova categoria inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na primeira página do assistente, selecione **Criar um pacote de instalação a partir de um arquivo**.

4. Na próxima página do assistente, especifique o nome do pacote de instalação e clique no botão **Procurar**.

   Uma janela padrão **Abrir** permite escolher um arquivo compactado para criar o pacote de instalação.

5. Selecione um arquivo morto localizado nos discos disponíveis.

   Você pode carregar um arquivo ZIP, CAB, TAR ou TAR.GZ. Não é possível criar um pacote de instalação a partir do arquivo SFX (arquivo de extração automática).

   Os arquivos são baixados no Servidor de Administração do Kaspersky Security Center Cloud Console.

   Se o Servidor de Administração detectar que o arquivo morto inclui o aplicativo Kaspersky, uma mensagem de erro será exibida. Você pode baixar pacotes de instalação para aplicativos Kaspersky nos Kaspersky Web Servers. Esta operação está disponível selecionando **Operações → Aplicativos Kaspersky → Versões atuais do aplicativo**.

6. Na próxima página do assistente, se o arquivo selecionado incluir vários arquivos executáveis, selecione um arquivo executável que deve ser executado para instalar o aplicativo usando o pacote de instalação criado.

7. Se desejar, especifique os parâmetros de linha de comando de um arquivo executável.

   Você pode especificar parâmetros da linha de comando, para instalar o aplicativo a partir do pacote de instalação em um modo silencioso. Consulte a documentação do fornecedor do aplicativo para obter detalhes sobre os parâmetros da linha de comando.

   A criação do pacote de instalação é iniciada.

   O assistente informa quando o processo é concluído.

   Se o pacote de instalação não for criado, é exibida uma mensagem de erro.

   No Kaspersky Security Center Cloud Console, o tamanho total de todos os pacotes de instalação no Servidor de Administração é limitado a 500 MB. Se no processo de criação de um pacote de instalação o limite total de tamanho for excedido, exclua os pacotes de instalação criados anteriormente. O tamanho de um pacote de instalação é exibido em suas propriedades.

8. Clique no botão **Concluir** para fechar o assistente.

O pacote de instalação personalizado criado é baixado para o Servidor de Administração. Após o download, o pacote de instalação aparece na lista de pacotes de instalação.

Na lista de pacotes de instalação, é possível visualizar as seguintes propriedades de um pacote de instalação personalizado:

- **Nome**. Nome do pacote de instalação personalizada.
- **Origem**. Nome do fornecedor do aplicativo.
- **Aplicativo**. Nome do aplicativo compactado no pacote de instalação personalizada.
- **Versão**. Versão do aplicativo.
- **Idioma**. Idioma do aplicativo compactado no pacote de instalação personalizada.
- **Tamanho (MB)**. Tamanho do pacote de instalação personalizado.
- **Sistema operacional**. Sistema operacional para o qual o pacote de instalação personalizado foi criado.

- **Criação**. Data de criação do pacote de instalação.
- **Modificação**. Data de modificação do pacote de instalação.
- **Tipo**. Aplicativo Kaspersky ou aplicativo de terceiros.

Na lista de pacotes de instalação, clicando no link com o nome de um pacote de instalação personalizado, você pode alterar os parâmetros da linha de comando e o nome do pacote de instalação personalizado.

Requisitos para um ponto de distribuição

Para processar até 10.000 dispositivos cliente, um ponto de distribuição deve atender aos seguintes requisitos mínimos (é fornecida uma configuração para teste):

- CPU: Intel® Core™ i7-7700 CPU, 3,60 GHz 4 núcleos.
- RAM: 8 GB.
- Espaço de armazenamento livre: 120 GB.

Além disso, um ponto de distribuição deve ter acesso à internet e deve sempre estar conectado.

Se quaisquer tarefas de instalação remota estiverem disponíveis no Servidor de Administração, o dispositivo com o ponto de distribuição também requer uma quantidade de espaço livre em disco que seja igual ao tamanho total dos pacotes de instalação a serem instalados.

Se uma ou múltiplas instâncias da tarefa para a instalação da atualização (patch) e de correção de vulnerabilidades estiverem pendentes no Servidor de Administração, o dispositivo com o ponto de distribuição também exigirá espaço livre adicional no disco que seja igual ao dobro do tamanho total de todos os patches a serem instalados.

Configurações de política do Agente de Rede

Para configurar uma política do Agente de Rede:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Agente de Rede.

   A janela de propriedades da política do Agente de Rede se abre.

Considere que para dispositivos baseados em Windows, macOS e Linux, várias configurações estão disponíveis.

Guia Geral

Nesta guia, você pode modificar o status da política e especificar a herança das configurações da política:

- No bloco **Status da política**, você pode selecionar um dos modos de política:
  - **Ativo**

- Inativo

  Se esta opção estiver selecionada, a política é habilitada, mas continua armazenada na pasta **Políticas**. Se necessário, a política pode ser habilitada.

- No grupo de configurações **Herança de configurações**, você pode configurar a herança de política:

  - Herdar configurações da política principal

    Se esta opção estiver ativada, os valores das configurações de política são herdados da política de grupo de nível superior e, portanto são bloqueados.

    Por padrão, esta opção está ativada.

  - Forçar herança de configurações nas políticas secundárias

    Se esta opção estiver ativada, após a aplicação das alterações da política, as seguintes ações serão realizadas:

    - Os valores das configurações da política serão propagados às políticas de subgrupos de administração, ou seja, às políticas secundárias.
    - No bloco **Herança de configurações** da seção **Geral** na janela Propriedades de cada política secundária, a opção **Herdar configurações da política principal** será automaticamente ativada.

    Se a opção estiver ativada, as configurações das políticas secundárias são bloqueadas.

    Por padrão, esta opção está desativada.

Guia Configuração de eventos

Esta guia permite configurar o registro de evento e a notificação de eventos. Os eventos são distribuídos conforme o nível de importância nas seguintes seções na guia **Configuração de eventos**:

- **Falha funcional**
- **Advertência**
- **Informações**

Em cada seção, a lista de tipos de eventos exibe os tipos de eventos e o prazo padrão de armazenamento de eventos no Servidor de Administração (em dias). Clicar no botão **Propriedades** lhe permite especificar as configurações do registro de eventos e as notificações sobre eventos selecionados na lista. Por padrão, as configurações de notificação comuns especificadas para todo o Servidor de Administração são usadas para todos os tipos de evento. Contudo, você pode alterar configurações específicas dos tipos de evento necessários.

Guia Configurações do aplicativo

Configurações

Na seção **Configurações**, você pode configurar a política do Agente de Rede:

- Distribuir os arquivos somente através dos pontos de distribuição

Se esta opção estiver marcada, os dispositivos cliente recuperam as atualizações somente através dos pontos de distribuição, não diretamente dos servidores de atualização.

Se esta caixa de seleção estiver desmarcada, os dispositivos cliente podem recuperar as atualizações de várias fontes: diretamente dos servidores de atualização e de uma pasta local ou de rede.

Por padrão, esta opção está desativada.

- **Tamanho máximo da fila de eventos, em MB**
- **O aplicativo tem permissão para recuperar os dados estendidos da política no dispositivo**

  O Agente de Rede instalado em um dispositivo gerenciado transfere informações sobre a política do aplicativo de segurança aplicada ao aplicativo de segurança (por exemplo, Kaspersky Endpoint Security for Windows). Você pode visualizar as informações transferidas na interface do aplicativo de segurança.

  O Agente de Rede transfere as seguintes informações:

  - Hora da entrega da política para o dispositivo gerenciado
  - Nome da política ativa ou de ausência temporária no momento da entrega da política ao dispositivo gerenciado
  - Nome e caminho completo para o grupo de administração que continha o dispositivo gerenciado no momento da entrega da política para o dispositivo gerenciado
  - Lista dos perfis de política ativos

    Você pode usar as informações para garantir que a política correta seja aplicada ao dispositivo e para fins de solução de problemas. Por padrão, esta opção está desativada.

- **Proteger serviço do Agente de Rede contra remoção ou interrupção não autorizada e impedir alterações nas configurações**

  Quando esta opção estiver ativado, após o Agente de Rede ter sido instalado em um dispositivo gerenciado, o componente não poderá ser removido ou reconfigurado sem os privilégios necessários. O serviço Agente de Rede não pode ser interrompido. Essa opção não tem efeito nos controladores de domínio.

  Ative esta opção para proteger o Agente de Rede em estações de trabalho operadas com direitos de administrador local.

  Por padrão, esta opção está desativada.

- **Usar senha de desinstalação**

  Caso esta opção esteja marcada, ao clicar no botão **Modificar**, será possível especificar a senha para o utilitário klmover e desinstalar remotamente o Agente de Rede.

  Por padrão, esta opção está desativada.

Repositórios

Na seção **Repositórios**, você pode selecionar os tipos de objetos cujos detalhes serão enviados do Agente de Rede para o Servidor de Administração. Se a modificação de algumas configurações nesta seção estiver bloqueada pela política do Agente de Rede, você não pode modificá-las. As configurações na seção **Repositórios** estão disponíveis somente em dispositivos que executam o Windows:

- **Detalhes dos aplicativos instalados**
- Incluir informações sobre patches

  As informações sobre os patches para os aplicativos instalados nos dispositivos cliente são enviadas ao Servidor de Administração. A ativação desta opção pode aumentar a carga no Servidor de Administração e DBMS, assim como causar volume aumentado do banco de dados.

  Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

- Detalhes das atualizações do Windows Update

  Se esta opção estiver marcada, as informações sobre as atualizações do Microsoft Windows Update que devem ser instaladas nos dispositivos clientes serão enviadas ao Servidor de Administração.

  Algumas vezes, mesmo se a opção estiver desativada, as atualizações são exibidas nas propriedades do dispositivo na seção **Atualizações disponíveis**. Pode acontecer se, por exemplo, os dispositivos da organização tiveram vulnerabilidades que poderiam ser corrigidas por estas atualizações.

  Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

- Detalhes das vulnerabilidades de software e das atualizações correspondentes

  Se essa opção estiver ativada, as informações sobre vulnerabilidades no software de terceiros (incluindo software da Microsoft), detectadas em dispositivos gerenciados e sobre atualizações de software para corrigir vulnerabilidades de terceiros (não incluindo o software da Microsoft) são enviadas ao Servidor de Administração.

  Selecionando esta opção (**Detalhes das vulnerabilidades de software e das atualizações correspondentes)** aumenta a carga da rede, a carga do disco do Servidor de Administração e o consumo de recurso pelo Agente de Rede.

  Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

  Para gerenciar atualizações de software da Microsoft, use a opção **Detalhes das atualizações do Windows Update**.

- **Detalhes do registro de hardware**

Atualizações e vulnerabilidades de software

Na seção **Atualizações e vulnerabilidades de software**, você pode configurar a pesquisa por atualizações Windows, assim como ativar a verificação de arquivos executáveis quanto a vulnerabilidades. As configurações na seção **Atualizações e vulnerabilidades de software** estão disponíveis somente em dispositivos que executam o Windows:

- Em **Permitir aos usuários gerenciar a instalação de atualizações do Windows Update**, você pode limitar as atualizações do Windows que os usuários podem instalar em seus dispositivos manualmente usando o Windows Update.

Em dispositivos que executam o Windows 10, se o Windows Update já tiver encontrado atualizações para o dispositivo, a nova opção selecionada em **Permitir aos usuários gerenciar a instalação de atualizações do Windows Update** será aplicada apenas depois que as atualizações encontradas forem instaladas.

Selecione um item na lista suspensa:

- **Permitir que os usuários instalem todas as atualizações do Windows Update**

  Os usuários podem instalar todas as atualizações do Microsoft Windows Update que são aplicáveis aos seus dispositivos.

  Selecione esta opção se você não quiser interferir na instalação das atualizações.

  Quando o usuário instala atualizações do Microsoft Windows Update manualmente, as atualizações podem ser baixadas de servidores da Microsoft e não do Servidor de Administração. Isso é possível se o Servidor de Administração ainda não tiver baixado as atualizações. Baixar atualizações dos servidores da Microsoft resulta em tráfego extra.

- **Permitir que os usuários instalem apenas atualizações do Windows Update aprovadas**

  Os usuários podem instalar todas as atualizações do Microsoft Windows Update que são aplicáveis aos seus dispositivos e que você aprovou.

  Por exemplo, pode ser necessário verificar primeiro a instalação das atualizações em um ambiente de teste, assegurar-se de que elas não interferem na operação dos dispositivos e, só então, permitir a instalação dessas atualizações aprovadas nos dispositivos cliente.

  Quando o usuário instala atualizações do Microsoft Windows Update manualmente, as atualizações podem ser baixadas de servidores da Microsoft e não do Servidor de Administração. Isso é possível se o Servidor de Administração ainda não tiver baixado as atualizações. Baixar atualizações dos servidores da Microsoft resulta em tráfego extra.

- **Não permitir que os usuários instalem atualizações do Windows Update**

  Os usuários não podem instalar atualizações do Microsoft Windows Update em seus dispositivos manualmente. Todas das atualizações aplicáveis são instaladas conforme configuradas por você.

  Selecione esta opção se você deseja gerenciar a instalação das atualizações centralmente.

  Por exemplo, pode ser necessário otimizar o agendamento da atualização para que a rede não fique sobrecarregada. Você pode agendar atualizações fora do horário para que não interfiram na produtividade dos usuários.

- No grupo de configurações **Modo de pesquisa do Windows Update**, você pode selecionar um modo de pesquisa de atualizações:

  - **Ativo**

Se essa opção estiver selecionada, o Servidor de Administração com suporte do Agente de Rede inicia uma solicitação ao Windows Update Agent no dispositivo cliente por uma fonte de atualização: Servidores do Windows Update ou WSUS. A seguir, o Agente de Rede passa as informações recebidas do Windows Update Agent para o Servidor de Administração.

A opção entra em vigor somente se **Conectar com o servidor de atualizações para atualizar dados** A opção da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* está selecionada.

Por padrão, esta opção está selecionada.

- **Passivo**

  Se você selecionar esta opção, o Agente de Rede passa informações ao Servidor de Administração periodicamente sobre atualizações obtidas na última sincronização do Windows Update Agent com a fonte de atualização. Se não for efetuada uma sincronização do Windows Update Agent com uma fonte de atualização, as informações sobre as atualizações no Servidor de Administração se tornam desatualizadas.

  Selecione esta opção se desejar obter atualizações do cache de memória da fonte de atualização.

- **Desativado**

  Se esta opção for selecionada, o Servidor de Administração não solicita qualquer informação sobre atualizações.

  Selecione esta opção se, por exemplo, quiser testar as atualizações no seu dispositivo local primeiro.

- **Verificar a vulnerabilidade dos arquivos executáveis ao executá-los**

  Se essa caixa de seleção estiver selecionada, as vulnerabilidades serão verificadas quando os arquivos executáveis forem executados.

  Por padrão, esta opção está desativada.

Gerenciamento de reinício

Na seção **Gerenciamento de reinício**, você pode especificar a ação a ser executada se o sistema operacional de um dispositivo gerenciado tiver de ser reiniciado para possibilitar o uso usar, instalação ou desinstalação correta de um aplicativo. As configurações na seção **Gerenciamento de reinício** estão disponíveis somente em dispositivos que executam o Windows:

- **Não reiniciar o sistema operacional**

  Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o sistema operacional automaticamente se necessário**

Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

  - **Repetir aviso a cada (min.)**

    Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

    Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

    Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  - **Forçar reinicialização após (min.)**

    Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

    Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

  A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

  Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

  Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

  Por padrão, esta opção está desativada.

Windows Desktop Sharing

Na seção **Windows Desktop Sharing**, você poderá ativar e configurar a auditoria das ações do administrador executadas em um dispositivo remoto quando o acesso à área de trabalho for compartilhado. As configurações na seção **Windows Desktop Sharing** estão disponíveis somente em dispositivos que executam o Windows:

- **Ativar auditoria**

Se a opção estiver marcada, a auditoria das ações do administrador no dispositivo remoto será ativada. Os registros de ações do administrador no dispositivo remoto são registrados:

- No log de eventos no dispositivo remoto
- Em um arquivo com a extensão syslog localizado na pasta de instalação do Agente de Rede no dispositivo remoto
- No banco de dados de eventos do Kaspersky Security Center Cloud Console

A auditoria das ações do administrador está disponível quando as seguintes condições são observadas:

- A licença de Gerenciamento de patches e vulnerabilidades está em uso
- O administrador tem o direito de iniciar o acesso compartilhado à área de trabalho do dispositivo remoto

Se esta opção estiver desmarcada, a auditoria das ações do administrador no dispositivo remoto será desativada.

Por padrão, esta opção está desativada.

- **Máscaras de arquivos para monitorar quando lidos**

  A lista contém máscaras de arquivos. Quando a auditoria é ativada, o aplicativo monitora a leitura do administrador de arquivos que correspondem às máscaras e salva informações sobre os arquivos lidos. A lista está disponível se a caixa de seleção **Ativar auditoria** for marcada. Você pode editar máscaras de arquivos e adicionar novas máscaras à lista. Cada nova máscara de arquivo deve ser especificada na lista em uma nova linha.

  Por padrão, são especificadas as seguintes máscaras de arquivos: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Máscaras de arquivos para monitorar quando modificados**

  A lista contém máscaras de arquivos no dispositivo remoto. Quando a auditoria é ativada, o aplicativo monitora alterações efetuadas pelo administrador em arquivos que correspondem a máscaras e salva informações sobre essas modificações. A lista está disponível se a caixa de seleção **Ativar auditoria** for marcada. Você pode editar máscaras de arquivos e adicionar novas máscaras à lista. Cada nova máscara de arquivo deve ser especificada na lista em uma nova linha.

  Por padrão, são especificadas as seguintes máscaras de arquivos: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Gerenciar patches e atualizações

Na seção **Gerenciar patches e atualizações**, você pode configurar o download e a distribuição das atualizações, assim como a instalação das patches nos dispositivos gerenciados: ative ou desative a opção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**.

Conectividade

A seção **Conectividade** inclui três subseções:

- **Rede**

- **Perfis de conexão**
- **Agendador de conexão**

Na subseção **Rede**, você pode configurar a conexão ao Servidor de Administração, ativar o uso de uma porta UDP e especificar o número da porta UDP.

- No grupo de configurações **Conexão ao Servidor de Administração**, você pode especificar as seguintes configurações:

  - Compactar o tráfego de rede

    Se esta opção estiver ativada, a velocidade de transferência de dados pelo Agente de Rede é aumentada através da redução da quantidade de informação a ser transferida e consequente carga inferior sobre o Servidor de Administração.

    A carga na CPU do computador cliente pode aumentar.

    Por padrão, esta caixa de seleção é marcada.

  - Abrir portas do Agente de Rede no firewall do Microsoft Windows

    Se esta opção estiver ativada, uma porta UDP é adicionada, necessária para o funcionamento do Agente de Rede, na lista de exclusão do Firewall do Microsoft Windows.

    Por padrão, esta opção está ativada.

  - Use o gateway de conexão em um ponto de distribuição (se disponível) sob as configurações de conexão padrão

    Se esta opção estiver marcada, o gateway de conexão no ponto de distribuição é usado sob as configurações especificadas nas propriedades do grupo de administração.

    Por padrão, esta opção está ativada.

- Usar porta UDP

  Se você desejar que os dispositivos gerenciados sejam conectados ao proxy da KSN através de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de **Porta UDP**. Por padrão, esta opção está ativada. A porta UDP padrão para se conectar ao servidor proxy KSN é 15111.

- Número da porta UDP

  Neste campo, é possível inserir o número da porta UDP. O número da porta padrão é 15000.

  É usado o sistema decimal para registros.

  Se um dispositivo cliente estiver executando o Windows XP Service Pack 2, o firewall integrado bloqueará a porta UDP 15000. Essa porta deve ser aberta manualmente.

- Usar o ponto de distribuição para forçar uma conexão com o Servidor de Administração

Selecione essa opção caso tenha selecionado **Executar servidor push** na janela de configurações do ponto de distribuição. Do contrário, o ponto de distribuição não atuará como um servidor push.

Na subseção **Perfis de conexão**, nenhum novo item pode ser adicionado à lista **Perfis de conexão do Servidor de Administração**. Por isso, o botão **Adicionar** estará inativo. Os perfis de conexão predefinidos também não podem ser modificados.

Na subseção **Agendador de conexão**, você pode especificar os intervalos de tempo durante os quais o Agente de Rede envia dados para o Servidor de Administração:

- **Conectar quando necessário**
- **Conectar-se nos intervalos de tempo especificados**

Na subseção **Agendador de conexão**, você pode especificar os intervalos de tempo durante os quais o Agente de Rede envia dados para o Servidor de Administração:

- Conectar quando necessário

  Se esta opção estiver selecionada, a conexão é estabelecida quando o Agente de Rede tem de enviar dados para o Servidor de Administração.

  Por padrão, esta opção está selecionada.

- Conectar-se nos intervalos de tempo especificados

  Se esta opção estiver selecionada, o Agente de Rede se conecta ao Servidor de Administração numa hora específica. Você pode adicionar vários períodos de tempo de conexão.

Sondagem da rede por pontos de distribuição

Na seção **Sondagem da rede por pontos de distribuição**, você pode configurar a amostragem automática da rede. As configurações de sondagem estão disponíveis somente em dispositivos que executam o Windows. Você pode usar as seguintes opções para ativar a sondagem e definir a frequência:

- Rede Windows

  Se essa opção estiver ativada, o ponto de distribuição pesquisará automaticamente a rede de acordo com a programação configurada clicando nos links **Definir agendamento da sondagem rápida** e **Definir agendamento da sondagem completa**.

  Se esta opção estiver ativada, o Servidor de Administração não realiza a sondagem da rede.

  Por padrão, esta opção está ativada.

- Intervalos de IPs

Se estiver opção estiver selecionada, o ponto de distribuição efetua automaticamente a sondagem de intervalos de IP de acordo com o agendamento configurado ao clicar no link **Definir agendamento da sondagem**.

Se essa opção estiver desmarcada, o ponto de distribuição não faz a sondagem dos intervalos de IP.

Por padrão, esta opção está desativada.

- Controladores de domínio

  Caso a opção esteja ativada, o ponto de distribuição realiza automaticamente a sondagem dos controladores de domínio de acordo com o agendamento configurado ao clicar no link **Definir agendamento da sondagem**.

  Caso essa opção esteja desativada, o ponto de distribuição não faz a sondagem dos controladores de domínio.

  A frequência de sondagem do controlador de domínio para as versões do Agente de Rede anteriores a 10.2 pode ser configurada no campo **Intervalo de sondagem (min.)**. O campo está disponível caso a opção esteja ativada.

  Por padrão, esta opção está desativada.

Configurações de rede para pontos de distribuição

Na seção **Configurações de rede para pontos de distribuição**, você pode especificar as configurações de acesso à Internet:

- **Usar o servidor proxy**
- **Endereço**
- **Número da porta**
- Ignorar servidor proxy para endereços locais

  Se esta opção estiver ativada, nenhum servidor proxy será usado para se conectar aos dispositivos na rede local.

  Por padrão, esta opção está desativada.

- Autenticação do servidor proxy

  Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

  Por padrão, esta caixa de seleção está desmarcada.

- **Nome do usuário**
- **Senha**

KSN Proxy (pontos de distribuição)

Na seção **KSN Proxy (pontos de distribuição)**, você pode configurar o aplicativo para usar o ponto de distribuição para encaminhar solicitações do KSN a partir dos dispositivos gerenciados:

- **Ativar o proxy da KSN no lado do ponto de distribuição**

  O serviço Proxy da KSN é executado no dispositivo que é usado como um ponto de distribuição. Use este recurso para redistribuir e otimizar o tráfego na rede.

  Esse recurso não tem suporte de dispositivos de ponto de distribuição executando Linux ou macOS.

  O ponto de distribuição envia as estatísticas da KSN, que são listadas na Declaração da Kaspersky Security Network, à Kaspersky. Por padrão, a Declaração da KSN está localizada em %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Por padrão, esta opção está desativada. A ativação desta opção somente tem efeito se a opção **Concordo em usar a Kaspersky Security Network** estiver ativada na janela de propriedades do Servidor de Administração.

  É possível atribuir um nó de um cluster ativo-passivo a um ponto de distribuição e habilitar o servidor proxy da KSN nesse nó.

- **Porta**

  O número da porta TCP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. O número da porta padrão é 13111.

- **Porta UDP**

  Se você desejar que os dispositivos gerenciados sejam conectados ao proxy da KSN através de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de **Porta UDP**. Por padrão, esta opção está ativada. A porta UDP padrão para se conectar ao servidor proxy KSN é 15111.

Comparação de configurações de política do Agente de Rede por sistemas operacionais

A tabela abaixo mostra quais configurações de política do Agente de Rede é possível usar para configurar o Agente de Rede com um sistema operacional específico.

Configurações de política do Agente de Rede: comparação por sistemas operacionais

Seção Política	Windows	macOS	Linux
Geral	✓	✓	✓
Configuração de eventos	✓	✓	✓
Configurações	✓	✓ Exceto a caixa de seleção **Usar senha de desinstalação**.	✓ Exceto a caixa de seleção **Usar senha de desinstalação**.
Repositórios	✓	–	✓

			As seguintes opções estão disponíveis: • Detalhes dos aplicativos instalados • Detalhes do registro de hardware
Atualizações e vulnerabilidades de software	✓	–	–
Gerenciamento de reinício	✓	–	–
Windows Desktop Sharing	✓	–	–
Gerenciar patches e atualizações	✓	–	–
Conectividade → Rede	✓	✓ Exceto a caixa de seleção **Abrir portas do Agente de Rede no firewall do Microsoft Windows**.	✓ Exceto a caixa de seleção **Abrir portas do Agente de Rede no firewall do Microsoft Windows**.
Conectividade → Agendador de conexão	✓	✓	✓
Sondagem da rede por pontos de distribuição	✓ As seguintes opções estão disponíveis: • **Rede Windows** • **Intervalos de IPs** • **Controladores de domínio** (Microsoft Active Directory)	–	✓ As seguintes opções estão disponíveis: • **Intervalos de IPs** • **Controladores de domínio** (Microsoft Active Directory, Samba como um Active Directory)
Configurações de rede para pontos de distribuição	✓	✓	✓
KSN Proxy (pontos de distribuição)	✓	–	✓

Configurações do pacote de instalação do Agente de Rede

Para configurar um pacote de instalação do Agente de Rede:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**.
   - No menu principal, vá para **Operações** → **Repositórios** → **Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Clique no link com o nome do pacote de instalação do Agente de Rede.

   A janela de propriedades do pacote de instalação do Agente de Rede é aberta. As informações na janela são agrupadas em guias e seções.

Geral

A seção **Geral** exibe informações gerais sobre o pacote de instalação:

- Nome do pacote de instalação
- Nome e versão do aplicativo para o qual o pacote de instalação foi criado
- Tamanho do pacote de instalação
- Data de criação do pacote de instalação
- Caminho para a pasta do pacote de instalação

Configurações

Esta seção apresenta as configurações necessárias para garantir o funcionamento adequado do Agente de Rede imediatamente após sua instalação. As configurações nesta seção estão disponíveis somente em dispositivos que executam o Windows.

No grupo de configurações da **Pasta de destino**, você pode selecionar a pasta do dispositivo cliente na qual o Agente de Rede será instalado.

- Instalar na pasta padrão

  Se esta opção estiver selecionada, o Agente de Rede será instalado na pasta <Unidade>:\Program Files\Kaspersky Lab\NetworkAgent. Se essa pasta não existir, ela será criada automaticamente.

  Por padrão, esta opção está selecionada.

- Instalar na pasta especificada

Se esta opção estiver selecionada, o Agente de Rede será instalado na pasta especificada no campo de entrada.

No seguinte grupo de configurações, você pode definir uma senha para uma tarefa de desinstalação remota do Agente de Rede:

- Usar senha de desinstalação

  Se esta opção estiver ativada, ao clicar no botão **Modificar**, você pode inserir a senha para desinstalar (somente disponível para o Agente de Rede em dispositivos que executam sistemas operacionais Windows).

  Por padrão, esta opção está desativada.

- **Status**

- Proteger serviço do Agente de Rede contra remoção ou interrupção não autorizada e impedir alterações nas configurações

  Quando esta opção estiver ativado, após o Agente de Rede ter sido instalado em um dispositivo gerenciado, o componente não poderá ser removido ou reconfigurado sem os privilégios necessários. O serviço Agente de Rede não pode ser interrompido. Essa opção não tem efeito nos controladores de domínio.

  Ative esta opção para proteger o Agente de Rede em estações de trabalho operadas com direitos de administrador local.

  Por padrão, esta opção está desativada.

- Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido

  Se esta caixa de controle estiver selecionada, todas as atualizações e patches baixados para o Agente de Rede serão instalados automaticamente.

  Se esta caixa de seleção estiver desmarcada, todas as atualizações e correções baixadas somente serão instaladas após você modificar o seu status para *Aprovado*. As atualizações e patches com o status *Indefinido* não serão instaladas.

  Por padrão, esta caixa de seleção está selecionada.

Conexão

Nesta seção, é possível configurar a conexão do Agente de Rede ao Servidor de Administração:

- **Usar porta UDP**

  Número da porta UDP

  Neste campo, é possível especificar a porta para conectar o Servidor de Administração com o Agente de Rede usando protocolo UDP.

  A porta UDP padrão é 15000.

- Abrir portas do Agente de Rede no Firewall do Microsoft Windows

Caso essa opção esteja ativada, as portas UDP usadas pelo Agente de Rede serão adicionadas na lista de exclusões do Firewall do Microsoft Windows.

Por padrão, esta opção está ativada.

- **Não usar servidor proxy**
- **Usar o servidor proxy**

  Endereço do servidor proxy

  Porta do servidor proxy
- Autenticação do servidor proxy

  Se esta caixa de seleção estiver marcada, você poderá especificar as credenciais para a autenticação do servidor proxy.

  Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

  Por padrão, esta opção está desativada.

  Nome do usuário

  Nome do usuário sob o qual a conexão ao servidor proxy é estabelecida.

  Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

  Senha

  Nome do usuário sob a qual a conexão ao servidor proxy é estabelecida.

  Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

Avançado

Na seção **Avançado**, você pode configurar a forma como o gateway de conexão é usado:

- **Conectar-se ao Servidor de Administração usando o gateway de conexão**
- **Ender. do gateway-conexão**
- Ativar modo dinâmico para VDI

  Se esta opção estiver ativada, o modo dinâmico para a Infraestrutura de Virtual Desktop Infrastructure (VDI) será habilitado para o Agente de Rede instalado em uma máquina virtual.

  Por padrão, esta opção está desativada.
- Otimizar as configurações para VDI

Se esta opção estiver ativada, os seguintes recursos estarão desativados nas configurações do Agente de Rede:

- Recuperar informações sobre o software instalado
- Recuperar informações sobre o hardware
- Recuperar informações sobre as vulnerabilidades detectadas
- Recuperar informações sobre as atualizações necessárias

Por padrão, esta opção está desativada.

Componentes adicionais

Nesta seção, você pode selecionar componentes adicionais para instalação simultânea com Agente de Rede.

Tags

A seção **Tags** exibe uma lista de palavras-chave (tags) que podem ser adicionadas aos dispositivos cliente após a instalação do Agente de Rede. Você pode adicionar e remover tags da lista, bem como renomeá-las.

Se a caixa de seleção estiver marcada ao lado da tag, essa será automaticamente adicionada aos dispositivos gerenciados durante a instalação do Agente de Rede.

Se a caixa de seleção estiver desmarcada ao lado da tag, essa não será automaticamente adicionada aos dispositivos gerenciados durante a instalação do Agente de Rede. Você pode adicionar manualmente essa tag aos dispositivos.

Ao remover uma tag da lista, ele será automaticamente removido de todos os dispositivos aos quais foi adicionada.

Histórico de revisões

Nesta seção, você poderá exibir o histórico de revisões do pacote de instalação. Você pode comparar revisões, exibir revisões, salvar revisões em um arquivo, e adicionar e editar descrições da revisão.

As configurações do pacote de instalação do Agente de Rede disponíveis para um sistema operacional específico são fornecidas na tabela abaixo.

Configurações do pacote de instalação do Agente de Rede

Seção da propriedade	Windows	Mac	Linux
Geral	✓	✓	✓
Configurações	✓	–	–
Conexão	✓	✓ * exceto a caixa de seleção **Abrir portas do Agente de Rede no Firewall do Microsoft Windows**	✓ * exceto a caixa de seleção **Abrir portas do Agente de Rede no Firewall do Microsoft Windows**
Avançado	✓	✓	✓
Componentes adicionais	✓	✓	✓

Tags	✓	✓ * exceto as regras de identificação automática	✓ * exceto as regras de identificação automática
Histórico de revisões	✓	✓	✓

Infraestrutura virtual

O Kaspersky Security Center Cloud Console é compatível com o uso de máquinas virtuais. Para proteger sua infraestrutura virtual, é necessário instalar o Agente de Rede em cada máquina virtual.

Dicas sobre como reduzir a carga em máquinas virtuais

Ao instalar o Agente de Rede em uma máquina virtual, você é aconselhado a considerar a desativação de alguns recursos do Kaspersky Security Center Cloud Console que parecem ser de um pouco uso para máquinas virtuais.

Ao instalar o Agente de Rede em uma máquina virtual ou em um modelo destinado para a geração de máquinas virtuais, recomendamos executar as seguintes ações:

- Se estiver executando uma instalação remota, na janela Propriedades do pacote de instalação do Agente de Rede na seção **Avançado**, selecione a opção **Otimizar as configurações para VDI**.
- Se você estiver executando uma instalação interativa por meio de um assistente, na janela assistente, selecione a opção **Otimizar as configurações do Agente de Rede para a infraestrutura virtual**.

Selecionar essas opções alterará as configurações do Agente de Rede para que os seguintes recursos permaneçam desativados por padrão (antes da política ser aplicada):

- Recuperar informações sobre o software instalado
- Recuperar informações sobre o hardware
- Recuperar informações sobre as vulnerabilidades detectadas
- Recuperar informações sobre as atualizações necessárias

Normalmente, aqueles recursos não são necessários em máquinas virtuais porque elas usam o software uniforme e o hardware virtual.

A desativação dos recursos é irreversível. Se algum dos recursos desativados for necessário, você pode ativá-lo através da política do Agente de Rede ou através das configurações locais do Agente de Rede. As configurações locais do Agente de Rede estão disponíveis através do menu de contexto do dispositivo relevante no Console de Administração.

Suporte de máquinas virtuais dinâmicas

O Kaspersky Security Center Cloud Console oferece suporte às máquinas virtuais dinâmicas. Se uma infraestrutura virtual tiver sido implementada na rede da organização, as máquinas virtuais dinâmicas (temporárias) podem ser usadas em determinados casos. As VMs dinâmicas são criadas sob nomes únicos com base em um modelo que foi preparado pelo administrador. O usuário trabalha em uma VM durante algum tempo, então, depois ser desligada, esta máquina virtual será removida da infraestrutura virtual. A máquina virtual com o Agente de Rede instalado também é adicionada ao banco de dados do Servidor de Administração. Depois de desligar esta máquina virtual, a entrada correspondente também deve ser removida do banco de dados do Servidor de Administração.

Para tornar funcional o recurso de remoção automática de entradas em máquinas virtuais, ao instalar o Agente de Rede em um modelo para máquinas virtuais dinâmicas, selecione a opção **Ativar modo dinâmico para VDI**:

- Para a instalação remota - na janela de propriedades do pacote de instalação do Agente de Rede (seção **Avançado**)
- Para a instalação interativa – No Assistente de instalação de Agente de Rede

Evite selecionar a opção **Ativar modo dinâmico para VDI** ao instalar o Agente de Rede em dispositivos físicos.

Se desejar que os eventos das máquinas virtuais dinâmicas sejam armazenados no Servidor de Administração durante algum tempo após essas máquinas virtuais serem removidas, então, na janela Propriedades do Servidor de Administração, na seção **Repositório de eventos**, selecione a opção **Armazenar eventos após a exclusão dos dispositivos** e especifique o período máximo de armazenamento para eventos (em dias).

Suporte para copiar máquinas virtuais

O Kaspersky Security Center Cloud Console oferece suporte à cópia de uma máquina virtual com o Agente de Rede instalado ou a criação de uma a partir de um modelo com o Agente de Rede instalado.

O Agente de Rede pode detectar automaticamente a cópia de máquinas virtuais nos seguintes casos:

- A opção **Ativar modo dinâmico para VDI** foi selecionada durante a instalação do Agente de Rede. Após cada reinicialização do sistema operacional, esta máquina virtual será reconhecida como um novo dispositivo, independentemente de ter sido copiada ou não.
- Um dos seguintes hypervisors está em uso: VMware™, HyperV®, ou Xen®: o Agente de Rede detecta a cópia da máquina virtual através das IDs alteradas do hardware virtual.

A análise das modificações no hardware virtual não é absolutamente confiável. Antes de aplicar este método amplamente, você deve testá-lo em um pequeno conjunto de máquinas virtuais da versão do hypervisor atualmente usado na sua organização.

Uso do Agente de Rede para Windows, macOS e Linux: comparativo

O Agente de Rede para macOS e Linux possui várias limitações funcionais em comparação com o Agente de Rede para Windows. A política do Agente de Rede e as configurações do pacote de instalação também diferem, dependendo do sistema operacional. A tabela a seguir compara os recursos do Agente de Rede e os cenários de uso disponíveis para os sistemas operacionais Windows, macOS e Linux.

Comparativo de recursos do Agente de Rede

Recurso do Agente de Rede	Windows	Linux	macOS
Instalação			
Instalação automática de atualizações e patches para o Agente de Rede	✓	–	–
Distribuir uma chave automaticamente	✓	✓	✓
Instalar manualmente, executando os instaladores do aplicativo em dispositivos	✓	✓	✓
Sincronização forçada	✓	✓	✓
Ponto de distribuição			
Sondagem da rede	✓ • Sondagem do conjunto de IPs • Sondagem da rede do Windows • Sondagem do controlador de domínio (Microsoft Active Directory)	✓ • Sondagem do conjunto de IPs • Sondagem do controlador de domínio (Microsoft Active Directory, Samba como um Active Directory)	–
Execução do Serviço de Proxy da KSN no lado do ponto de distribuição	✓	–	–
Baixar atualizações via servidores de atualização Kaspersky para os repositórios de pontos de distribuição que distribuem atualizações para dispositivos gerenciados	✓	✓	– Os dispositivos de ponto de distribuição executando macOS não podem baixar atualizações dos servidores de atualização da Kaspersky. Se um ou mais dispositivos executando macOS estiverem dentro do escopo da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a tarefa será concluída com o status *Falha*, mesmo se for concluída com êxito em todos os dispositivos Windows.
Instalação push de aplicativos	✓	Restrito: não é possível realizar	

		instalação push em dispositivos Windows usando pontos de distribuição Linux.	
Gerenciamento de aplicativos de terceiros			
Instalação remota de aplicativos em dispositivos	✓	–	–
Atualizações de software	✓	–	–
Configurar as atualizações do sistema operacional em uma política de Agente de Rede	✓	–	–
Exibir informações sobre as vulnerabilidades do software	✓	–	–
Verificar os aplicativos quanto a vulnerabilidades	✓	–	–
Inventário de software instalado nos dispositivos	✓	–	–
Máquinas virtuais			
Instalar o Agente de Rede em uma máquina virtual	✓	✓	✓
As configurações de optimização da infraestrutura de desktop virtual (VDI)	✓	✓	✓
Suporte de máquinas virtuais dinâmicas	✓	✓	✓
Outro			
Auditoria de ações em um dispositivo cliente remoto usando o Windows Desktop Sharing	✓	–	–
Gerenciar reinícios de dispositivos	✓	–	–
Gerenciador de conexões	✓	✓	✓
Conexão remota à Área de trabalho de um dispositivo cliente	✓	–	–

As seções a seguir são exibidas nas propriedades do ponto de distribuição, mas os recursos correspondentes não são compatíveis com o Agente de Rede para macOS:

- Fonte de atualizações
- Servidor Proxy da KSN
- Domínios do Windows
- Active Directory
- Intervalos de IP
- Avançado
- Estatísticas

Especificando configurações para instalação remota em dispositivos Unix

Ao instalar um aplicativo em um dispositivo Unix usando uma tarefa de instalação remota, você pode especificar configurações específicas do Unix para a tarefa. Essas configurações estão disponíveis nas propriedades da tarefa depois da tarefa ser criada.

Para especificar configurações específicas do Unix para uma tarefa de instalação remota:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique no nome da tarefa de instalação remota para a qual deseja especificar as configurações específicas do Unix.

   A janela de propriedades da tarefa é aberta.
3. Acesse **Configurações do aplicativo** → **Configurações Unix específicas**.
4. Especificar as seguintes configurações:

   - Defina uma senha para a conta raiz (apenas para implementação via SSH)

     Se o comando `sudo` não puder ser usado no dispositivo de destino sem especificar a senha, selecione esta opção e, em seguida, especifique a senha para a conta raiz. Kaspersky Security Center Cloud Console transmite a senha de forma criptografada para o dispositivo de destino, descriptografa a senha e inicia o procedimento de instalação em nome da conta raiz com a senha especificada.

     Kaspersky Security Center Cloud Console não usa a conta ou a senha especificada para criar uma conexão SSH.

   - Especifique o caminho para uma pasta temporária com permissões de execução no dispositivo de destino (apenas para implementação via SSH)

Se o diretório/tmp no dispositivo de destino não tiver permissão de execução, selecione esta opção e, a seguir, especifique o caminho para o diretório com a permissão de execução. O Kaspersky Security Center Cloud Console usa o diretório especificado como um diretório temporário para acessar via SSH. O aplicativo coloca o pacote de instalação no diretório e executa o procedimento de instalação.

5. Clique no botão **Salvar**.

As configurações de tarefa especificadas são salvas.

Substituição de aplicativos de segurança de terceiros

A Instalação de aplicativos de segurança Kaspersky através do Kaspersky Security Center Cloud Console pode necessitar a remoção de software de terceiros incompatível com o aplicativo sendo instalado. O Kaspersky Security Center Cloud Console fornece vários modos de remover os aplicativos de terceiros.

Remoção de aplicativos incompatíveis ao configurar a instalação remota de um aplicativo

Você pode ativar a opção **Desinstalar automaticamente aplicativos incompatíveis** ao configurar a instalação remota de um aplicativo de segurança. Essa opção está disponível no Assistente de Implementação da Proteção. Quando esta opção está ativada, o Kaspersky Security Center Cloud Console remove aplicativos incompatíveis antes de instalar um aplicativo de segurança em um dispositivo gerenciado.

Remover aplicativos incompatíveis através de uma tarefa dedicada

Para remover aplicativos incompatíveis através de uma tarefa, use a tarefa **Desinstalar o aplicativo remotamente**. Esta tarefa deve ser executada nos dispositivos antes da execução da tarefa de instalação do aplicativo de segurança. Por exemplo, na tarefa de instalação, você pode selecionar o tipo de agendamento **Na conclusão de outra tarefa** onde a outra tarefa for **Desinstalar o aplicativo remotamente**.

Este método da desinstalação é útil quando o instalador do aplicativo de segurança não puder remover apropriadamente um aplicativo incompatível.

Opções para a instalação manual de aplicativos

É possível instalar o Agente de Rede em dispositivos localmente sem precisar recorrer ao Kaspersky Security Center Cloud Console. Para fazer isso, crie um pacote de instalação independente para o Agente de Rede conforme descrito no tópico a seguir: Criação de pacotes de instalação independentes. Transfira o pacote para o dispositivo cliente e instale. Depois que a instalação do Agente de Rede estiver concluída, será possível usar o dispositivo como um ponto de distribuição.

Assistente de implementação da proteção

Para instalar os aplicativos da Kaspersky, você pode usar o assistente de Implementação da proteção. O assistente de Implementação da proteção permite a instalação remota de aplicativos por meio de pacotes de instalação especialmente criados ou diretamente de um pacote de distribuição.

O Assistente de implementação de proteção executa as seguintes ações:

- Baixa um pacote de instalação para implementação do aplicativo (se não foi criado anteriormente). O pacote de instalação está localizado em **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**. Você pode usar esse pacote de instalação para instalação do aplicativo no futuro.
- Cria e executa uma tarefa de instalação remota para dispositivos específicos ou para um grupo de administração. A tarefa de instalação remota recém-criada é armazenada na seção **Tarefas**. Você pode iniciar essa tarefa manualmente mais tarde. O tipo de tarefa é **Instalar o aplicativo remotamente**.

Iniciar o assistente de implementação da proteção

Para iniciar o assistente de implementação da proteção manualmente,

No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Assistente de Implementação de Proteção**.

O assistente de implementação da proteção é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

Etapa 1. Seleção do pacote de instalação

Selecione o pacote de instalação do aplicativo que deseja instalar.

Se o pacote de instalação do aplicativo necessário não estiver listado, clique no botão **Adicionar** e selecione o aplicativo na lista.

Etapa 2. Seleção de versão do Agente de Rede

Se tiver selecionado o pacote de instalação de um aplicativo que não o Agente de Rede, você também precisará instalar o Agente de Rede, que conecta o aplicativo ao Servidor de Administração do Kaspersky Security Center.

Selecione a versão mais recente do Agente de Rede.

Etapa 3. Seleção de dispositivos

Especifique uma lista de dispositivos nos quais o aplicativo será instalado:

- Instalar em dispositivos gerenciados

  Se esta opção estiver selecionada, a tarefa de instalação remota para um grupo de dispositivos será criada.

- Selecionar dispositivos para a instalação

A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

Etapa 4. Especificação das configurações de tarefa de instalação remota

Na página **Configurações da tarefa de "instalação remota"**, especifique as configurações para a instalação remota do aplicativo.

No grupo de configurações **Forçar download do pacote de instalação**, especifique como os arquivos que são necessários para instalar um aplicativo são distribuídos nos dispositivos cliente:

- **Usando o Agente de Rede**

  Se esta opção de seleção estiver ativada, os pacotes de instalação são entregues aos dispositivos cliente pelo Agente de Rede instalado neles.

  Caso esta opção estiver desativada, os pacotes de instalação serão entregues usando as ferramentas do sistema operacional dos dispositivo cliente.

  Recomendamos que você ative esta opção se a tarefa tiver sido atribuída a dispositivos com o Agente de Rede instalado.

  Por padrão, esta opção está ativada.

- **Usando recursos do sistema operacional através de pontos de distribuição**

  Se esta opção estiver ativada, os pacotes de instalação serão transmitidos para os dispositivos cliente usando as ferramentas do sistema operacional, através dos pontos de distribuição. Você pode selecionar esta opção se houver, no mínimo, um ponto de distribuição na rede.

  Se opção **Uso do Agente de Rede** estiver ativada, os arquivos serão entregues pelas ferramentas do sistema operacional, apenas se os recursos do Agente de Rede estiverem indisponíveis.

  Por padrão, esta opção está ativada para as tarefas de instalação remotas que são criadas em um Servidor de Administração virtual.

Defina as configurações adicionais:

Não reinstalar o aplicativo se ele já estiver instalado

Se esta opção estiver ativada, o aplicativo selecionado não será reinstalado se já estiver instalado neste dispositivo cliente.

Se esta opção não estiver ativada, o aplicativo será instalado de qualquer forma.

Por padrão, esta opção está ativada.

Etapa 5. Gerenciamento de reinício

Especifique a ação a ser executada se o sistema operacional precisar ser reiniciado quando você instalar o aplicativo:

- **Não reiniciar o dispositivo**

  Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

  - **Repetir aviso a cada (min.)**

    Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

    Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

    Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  - **Reiniciar após (min.)**

    Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

    Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

Etapa 6. Remoção de aplicativos incompatíveis antes de instalação

Esta etapa só estará presente se o aplicativo implementado for incompatível com outros aplicativos.

Selecione a opção se quiser que o Kaspersky Security Center Cloud Console remova automaticamente aplicativos incompatíveis com o aplicativo implementado.

A lista de aplicativos incompatíveis também é exibida.

Se você não marcar esta opção, o aplicativo será instalado apenas em dispositivos que não têm aplicativos incompatíveis.

Etapa 7. Movimentação de dispositivos para dispositivos gerenciados

Especifique se os dispositivos devem ser movidos para um grupo de administração depois da instalação do Agente de Rede.

- **Não migrar dispositivos**

  Os dispositivos permanecem nos grupos nos quais eles estão atualmente localizados. Os dispositivos que não foram colocados em nenhum grupo continuam não atribuídos.

- **Migrar dispositivos não atribuídos para o grupo**

  Os dispositivos são movidos para o grupo de administração selecionado.

A opção **Não migrar dispositivos** está marcada por padrão. Por motivos de segurança, você pode desejar mover os dispositivos manualmente.

Etapa 8. Seleção de contas para acessar dispositivos

Se necessário, adicione as contas que serão usadas para iniciar a tarefa de instalação remota:

- **Nenhuma conta necessária (Agente de Rede instalado)**

Se essa caixa de seleção estiver selecionada, você não precisará especificar uma conta sob a qual o instalador do aplicativo será executado. A tarefa será executada sob a conta sob a qual o serviço do Servidor de Administração está sendo executado.

Se o Agente de Rede não tiver sido instalado em dispositivos cliente, esta opção não estará disponível.

- Conta necessária (Agente de Rede não é usado)

  Selecione esta opção se o Agente de Rede não estiver instalado nos dispositivos aos quais você atribui a tarefa de instalação remota. Neste caso, é possível especificar uma conta de usuário para instalar o aplicativo.

  Para especificar a conta de usuário sob a qual o instalador do aplicativo será executado, clique no botão **Adicionar** botão, selecione **Conta local** e, em seguida, especifique as credenciais da conta de usuário.

  É possível especificar várias contas de usuário se, por exemplo, nenhuma delas tiver todos os direitos necessários em todos os dispositivos para os quais você atribui a tarefa. Nesse caso, todas as contas adicionadas são usadas para executar a tarefa, em ordem consecutiva, de cima para baixo.

Etapa 9. Início da instalação

Essa página é a última etapa do assistente. Nesta etapa, a **Tarefa de instalação remota** foi criada e configurada com sucesso.

Por padrão, a opção **Executar a tarefa após a conclusão do assistente** não está selecionada. Caso esta opção seja selecionada, a **Tarefa de instalação remota** será iniciada imediatamente após a conclusão do assistente. Caso esta opção não seja marcada, a **Tarefa de instalação remota** não será iniciada. Você pode iniciar essa tarefa manualmente mais tarde.

Clique em **OK** para concluir a etapa final do assistente de implementação da proteção.

Configurações de rede para interação com serviços externos

O Kaspersky Security Center Cloud Console usa as configurações de rede a seguir para interagir com serviços externos.

Configurações de rede

Configurações de rede	Endereço	Descrição
Porta: 443 Protocolo: HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	Ativação do aplicativo.
Porta: 443 Protocolo: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com	Atualização de bancos de dados, módulos de software e aplicativos da Kaspersky.

	https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	
Porta: 443 Protocolo: HTTPS	https://downloads.upd.kaspersky.com	• Atualização de bancos de dados, módulos de software e aplicativos da Kaspersky. • Verificar se os servidores da Kaspersky estão acessíveis. Antes de baixar os bancos de dados e módulos de software da Kaspersky, o Kaspersky Security Center Cloud Console verifica se os servidores da Kaspersky estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos.
Porta: 80 Protocolo: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com	Atualização de bancos de dados, módulos de software e aplicativos da Kaspersky.

	http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	
Porta: 443 Protocolo: HTTPS	ds.kaspersky.com	Uso da Kaspersky Security Network.
Porta: 443, 1443 Protocolo: HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Uso da Kaspersky Security Network.
Protocolo: HTTPS	click.kaspersky.com redirect.kaspersky.com	Como seguir os links da interface.
Porta: 80 Protocolo: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Infraestrutura de Chave Pública (PKI).
Porta: 443 Protocolo: HTTPS	https://ipm-klca.kaspersky.com	Informativos de marketing.

Preparar um dispositivo executando o Astra Linux no modo de ambiente de software fechado para a instalação do Agente de Rede

Antes da instalação do Agente de Rede em um dispositivo executando o Astra Linux no modo de ambiente de software fechado, execute dois procedimentos de preparação: o mencionado nas instruções abaixo e as etapas gerais de preparação para qualquer dispositivo Linux.

Antes de iniciar:

- Verifique e confirme se o dispositivo no qual deseja instalar o Agente de Rede para Linux está executando uma das distribuições Linux compatíveis.
- Baixe o arquivo de instalação do Agente de Rede necessário do site da Kaspersky.

Execute os comandos fornecidos nesta instrução em uma conta com privilégios de acesso root.

Para preparar um dispositivo executando o Astra Linux no modo de ambiente de software fechado para a instalação do Agente de Rede:

1. Abra o arquivo /etc/digsig/digsig_initramfs.conf e especifique a seguinte configuração:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Na linha de comando, execute o seguinte comando para instalar o pacote de compatibilidade:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Crie um diretório para a chave do aplicativo:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Coloque a chave do aplicativo /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg no diretório criado na etapa anterior:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Se o kit de distribuição do Kaspersky Security Center Cloud Console não incluir a chave do aplicativo kaspersky_astra_pub_key.gpg, você poderá baixá-lo clicando no link: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Atualize os discos RAM:

   ```
   update-initramfs -u -k all
   ```

   Reinicialize o sistema.

6. Execute as etapas de preparação comuns para qualquer dispositivo Linux.

O dispositivo está preparado. Agora você pode prosseguir para a instalação do Agente de Rede.

Preparar um dispositivo Linux e instalar o Agente de Rede em um dispositivo Linux remotamente

A instalação do Agente de Rede compreende duas etapas:

- Preparação de um dispositivo Linux
- Instalação remota do Agente de Rede

Preparação de um dispositivo Linux

Para preparar um dispositivo executando no Linux para a instalação remota do Agente de Rede:

1. Certifique-se de que o software a seguir está instalado no dispositivo Linux de destino:
   - Sudo
   - Intérprete de linguagem Perl versão 5.10 ou posterior
2. Testar a configuração do dispositivo:
   a. Verifique se você pode conectar-se ao dispositivo através de um cliente SSH (como PuTTY).

      Se você não puder conectar-se ao dispositivo, abra o arquivo /etc/ssh/sshd_config e assegure-se de que as seguintes configurações têm os respetivos valores listados abaixo:

      `PasswordAuthentication no`

      `ChallengeResponseAuthentication yes`

      > Não modifique o arquivo /etc/ssh/sshd_config caso possa se conectar ao dispositivo sem problemas. Caso contrário, poderá haver falha de autenticação SSH ao executar uma tarefa de instalação remota.

      Salve o arquivo (se necessário) e reinicie o serviço SSH usando o comando `sudo service ssh restart`.

   b. Desative a senha sudo para a conta do usuário sob a qual o dispositivo deve ser conectado.

   c. Use o comando `visudo` no sudo para abrir o arquivo de configuração sudoers.

      No arquivo que você abriu, encontre a linha que começa com `%sudo` (ou com `%wheel` se você estiver usando o sistema operacional CentOS). Nesta linha, especifique o seguinte: <`username` > `ALL = (ALL) NOPASSWD: ALL`. Neste caso, o < `username` > é a conta de usuário que deve ser usada para a conexão de dispositivo usando o SSH. Caso esteja usando o sistema operacional Astra Linux, no arquivo /etc/sudoers, adicione a última linha com o seguinte texto: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Salve o arquivo sudoers e, a seguir, feche-o.

   e. Conecte-se novamente ao dispositivo pelo SSH, verifique e confirme se o serviço Sudo não solicita a inserção de uma senha. Será possível fazer isso com o uso do comando `sudo whoami`.
3. Abra o arquivo /etc/systemd/logind.conf e proceda de uma das seguintes formas:
   - Especifique 'no' como valor para a configuração de KillUserProcesses: `KillUserProcesses=no`.
   - Para a configuração de KillExcludeUsers, digite o nome de usuário da conta sob a qual a instalação remota será executada, por exemplo `KillExcludeUsers=root`.

Caso o dispositivo de destino esteja executando o Astra Linux, adicione a string export `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` no arquivo `/home/<nome de usuário>/.bashrc`, onde `<nome de usuário>` é a conta de usuário que deve ser usada para a conexão do dispositivo com o uso do SSH.

Para aplicar a configuração alterada, reinicie o dispositivo Linux ou execute o comando a seguir:

```
$ sudo systemctl restart systemd-logind.service
```

4. Caso queira instalar o agente de rede em dispositivos com o sistema operacional SUSE Linux Enterprise Server 15, instale o pacote insserv-compat primeiro para configurar o agente de rede.

5. Se você quiser instalar o Agente de Rede em dispositivos com o sistema operacional Astra Linux em execução no modo de ambiente de software fechado, execute as etapas adicionais para preparar os dispositivos Astra Linux.

Instalação remota do Agente de Rede

Para instalar o Agente de Rede em dispositivos Linux remotamente:

1. Baixar e criar um pacote de instalação:

   a. Antes da instalação no dispositivo, assegure-se que ele já tenha todas as dependências (programas e bibliotecas) instaladas para este pacote.

   Você pode exibir as dependências para cada pacote por si só, usando utilitários que são específicos para a distribuição Linux na qual o pacote deve ser instalado. Para obter mais detalhes sobre os utilitários, consulte a documentação de seu sistema operacional.

   b. Baixe o pacote de instalação do Agente de Rede usando a interface do aplicativo ou no site da Kaspersky.

   c. Para criar um pacote de instalação remota, use os seguintes arquivos:

   - klnagent.kpd
   - akinstall.sh
   - Pacote .deb ou .rpm para Agente de Rede

2. Criar uma tarefa de instalação remota com as seguintes configurações:

   - Na página **Configurações** do Assistente para novas tarefas, marque a caixa de seleção **Uso dos recursos do sistema operacional por meio do Servidor de Administração**. Limpar todas as outras caixas de seleção.
   - Na página **Selecionar uma conta para executar a tarefa**, especifique as configurações da conta de usuário usadas para a conexão do dispositivo através de SSH.

3. Executar a tarefa de instalação remota. Use a opção para o comando `su` para preservar o ambiente: `-m, -p, --preserve-environment`.

Um erro poderia ser retornado se você instalar o Agente de Rede com SSH nos dispositivos que executam versões do Fedora anteriores a 20. Neste caso, para instalação bem-sucedida do Agente de Rede, desative a opção Defaults requiretty (inclua-a na sintaxe de comentário para removê-la do código analisado) no arquivo /etc/sudoers. Para obter uma descrição detalhada da condição da opção Defaults requiretty, que pode causar problemas durante a conexão através de SSH, consulte o site do Bugzilla bugtracker.

Gerenciamento de Dispositivos Móveis

O gerenciamento da proteção de dispositivos móveis por meio do Kaspersky Security Center Cloud Console é executado usando o recurso Gerenciamento de Dispositivos Móveis. Se você pretende gerenciar dispositivos móveis de propriedade dos funcionários da sua organização, ative o Gerenciamento de Dispositivos Móveis.

O Gerenciamento de Dispositivos Móveis permite gerenciar os dispositivos Android dos funcionários. A proteção é fornecida pelo aplicativo móvel Kaspersky Endpoint Security for Mobile, instalado nos dispositivos. Este aplicativo móvel garante a proteção de dispositivos móveis contra ameaças da web, vírus e outros programas que representam ameaças.

Para obter informações sobre a implementação de proteção e gerenciamento de dispositivos móveis, consulte a Ajuda do Kaspersky Security for Mobile.

Recursos de detecção e resposta

Esta seção contém informações sobre as soluções da Kaspersky que podem ser integradas ao Kaspersky Security Center Cloud Console para adicionar recursos de detecção e resposta ao console.

Sobre os recursos de detecção e resposta

O Kaspersky Security Center Cloud Console pode integrar recursos de outras soluções da Kaspersky na interface do console. Por exemplo, é possível adicionar os recursos de detecção e resposta à funcionalidade do Kaspersky Security Center Cloud Console.

As soluções de detecção e resposta são projetadas para proteger a infraestrutura de TI de uma organização contra ciberameaças complexas. A funcionalidade da solução combina a detecção automática de ameaças com a capacidade de responder a essas ameaças para resistir a ataques complexos, incluindo novos exploits, ransomware, ataques sem arquivo e métodos que usam ferramentas legítimas de sistema.

É possível integrar as seguintes soluções:

- Kaspersky Endpoint Detection and Response Optimum

  Depois que um aplicativo Kaspersky Endpoint Protection Platform (também conhecido como EPP) detecta uma ameaça, o Kaspersky Security Center Cloud Console adiciona um novo alerta na lista de alertas. Um alerta contém informações detalhadas sobre a ameaça detectada e permite a análise e investigação da ameaça. Além disso, é possível visualizar a ameaça criando um gráfico da cadeia de desenvolvimento de ameaças. O gráfico descreve as fases de implementação do ataque detectado ao longo do tempo.

  Como resposta, é possível escolher uma das ações de resposta predefinidas, por exemplo, isolar um objeto não confiável, isolar um dispositivo comprometido da rede ou criar uma regra de prevenção de execução para um objeto não confiável.

  Para obter informações sobre a ativação da solução, consulte a documentação do Kaspersky Endpoint Detection and Response Optimum.

- Kaspersky Managed Detection and Response

  Depois que um aplicativo Kaspersky EPP detecta uma ameaça, o Kaspersky Security Center Cloud Console adiciona um novo incidente à lista de incidentes. Um incidente contém informações detalhadas sobre a ameaça detectada. Os analistas de MDR Security Operation Center (SOC) da Kaspersky ou de uma empresa terceirizada investigam os incidentes e oferecem respostas para resolvê-los. Você pode aceitar ou rejeitar as medidas oferecidas manualmente, ou habilitar a opção de aceitar automaticamente todas as respostas.

  Para obter informações sobre a ativação da solução, consulte a documentação do Kaspersky Managed Detection and Response.

- Kaspersky Endpoint Detection and Response Expert

  Essa é uma solução para organizações que possuem uma equipe de analistas de SOC. As ameaças detectadas são registradas como alertas ou incidentes que podem ser atribuídos aos analistas de SOC para investigação. O Kaspersky Endpoint Detection and Response Expert fornece informações detalhadas sobre cada alerta ou incidente, assim como as ferramentas para o gerenciamento de alertas e incidentes, caça a ameaças e desenvolvimento de regras personalizadas. Os analistas ou diretores de segurança de SOC podem selecionar manualmente as ações de resposta, ou as medidas de resposta automatizadas predefinidas podem ser adotadas.

  Para obter informações sobre a ativação da solução, consulte a documentação do Kaspersky Endpoint Detection and Response Expert.

Mudanças na interface após a integração dos recursos de detecção e resposta

As seguintes soluções da Kaspersky fornecem recursos de detecção e resposta que podem ser integrados na interface do Kaspersky Security Center Cloud Console:

- Kaspersky Endpoint Detection and Response (EDR) Optimum
- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response (EDR) Expert

A tabela a seguir lista as alterações feitas pelas soluções na interface do Kaspersky Security Center Cloud Console após a integração.

Alterações de interface feitas pelas soluções integradas da Kaspersky

Solução	Alterações no Kaspersky Security Center Cloud Console
Kaspersky EDR Optimum	Adiciona os seguintes elementos: • Seção **Alertas** (**Monitoramento e relatórios** → **Alertas**). Os alertas detectados por essa solução estão listados na guia **Optimum**. • Um widget em **Painel** (**Monitoramento e relatórios** → **Painel**).
Kaspersky MDR	Adiciona os seguintes elementos: • Seção **MDR** (**Monitoramento e relatórios** → **MDR**). • A opção **Exibir recursos MDR** (**Configurações** → **Opções da interface** → **Exibir recursos MDR**). • Um widget em **Painel** (**Monitoramento e relatórios** → **Painel**).
Kaspersky EDR Expert	Adiciona os seguintes elementos: • Seção **Alertas** (**Monitoramento e relatórios** → **Alertas**). Os alertas detectados por essa solução estão listados na guia **Expert**. • Seção **Incidentes** (**Monitoramento e relatórios** → **Incidentes**). • Seção **Caça a ameaças** (**Monitoramento e relatórios** → **Caça a ameaças**). • Seção **Regras personalizadas** (**Monitoramento e relatórios** → **Regras personalizadas**). • Configurações gerais do Kaspersky EDR Expert (**Configurações** → **Integração** → **Kaspersky EDR Expert**). • Widgets em **Painel** (**Monitoramento e relatórios** → **Painel**).

Detectando dispositivos em rede e criando grupos de administração

Esta seção descreve a pesquisa e descoberta de dispositivos em rede, bem como a criação grupos de administração para esses dispositivos.

O Kaspersky Security Center Cloud Console permite localizar dispositivos com base em critérios especificados. Você pode salvar os resultados da pesquisa em um arquivo de texto.

O recurso de pesquisa e localização permite localizar os seguintes dispositivos:

- Dispositivos gerenciados nos grupos de administração do Servidor de administração do Kaspersky Security Center Cloud Console e seus Servidores de administração secundários.
- Dispositivos não atribuídos gerenciados pelo Servidor de administração do Kaspersky Security Center Cloud Console e seus Servidores de administração secundários.

Cenário: Localizar dispositivos na rede

Você deve executar a descoberta de dispositivos antes da implementação inicial dos aplicativos de segurança. Quando todos os dispositivos em rede são descobertos, você pode adquirir informações sobre eles e gerenciá-los por meio de políticas. Amostragens de rede regulares são necessárias para descobrir se há algum novo dispositivo e se os dispositivos anteriormente descobertos ainda estão na rede.

Quando você conclui o cenário, a descoberta de dispositivos é configurada e será conduzida de acordo com o agendamento especificado.

Pré-requisitos

No Kaspersky Security Center Cloud Console, a descoberta de dispositivos é realizada por pontos de distribuição. Antes de começar, faça o seguinte:

- Decida quais dispositivos atuarão como pontos de distribuição.
- Instale Agentes de Rede nos dispositivos escolhidos.
- Para atribuir manualmente os dispositivos para agirem como ponto de distribuição.

Fases

O cenário continua em estágios:

1. **Escolher tipos de descoberta**

   Decida quais tipos de descoberta deseja usar regularmente.

2. **Configurar amostragens**

   Nas propriedades de cada ponto de distribuição, ative e configure os tipos de sondagem de rede escolhidos: sondagem de rede do Windows, sondagem do controlador de domínio ou sondagem de intervalo de IPs. Verifique se o agendamento da amostragem atende às necessidades da sua organização.

   Se os dispositivos em rede estiverem incluídos em um domínio, recomenda-se usar a sondagem do controlador de domínio.

3. **Configuração de regras para adicionar dispositivos descobertos a grupos de administração (opcionais)**

   Se os novos dispositivos aparecerem na sua rede, eles serão descobertos durante as amostragens regulares e automaticamente incluídos no grupo **Dispositivos não atribuídos**. Se quiser, você poderá configurar as regras para mover esses dispositivos para o grupo **Dispositivos gerenciados**. Você também pode estabelecer regras de retenção.

   Se você ignorar esta etapa de configuração de regra, todos os dispositivos recentemente descobertos serão movidos para o grupo **Dispositivos não atribuídos** e ficarão lá. Se quiser, você poderá mover esses dispositivos para o grupo **Dispositivos gerenciados** manualmente. Se mover os dispositivos para o grupo **Dispositivos gerenciados**, você poderá analisar informações sobre cada dispositivo e decidir se deseja movê-lo para um grupo de administração e, nesse caso, para qual grupo.

Quando uma operação de pesquisa de rede estiver concluída, verifique se os dispositivos recém-descobertos estão organizados de acordo com as regras configuradas. Se nenhuma regra for configurada, os dispositivos permanecerão no grupo **Dispositivos não atribuídos**.

Sondagem da rede

As informações sobre a estrutura da rede e os dispositivos nessa rede são recebidas pelo Kaspersky Security Center Cloud Console por meio de sondagem regular da rede Windows, intervalos de IP, controlador de domínio Microsoft Active Directory e controlador de domínio Samba. Para um controlador de domínio Samba, o Samba 4 é usado como um controlador de domínio do Active Directory. A amostragem da rede pode ser iniciada manualmente ou automaticamente, de acordo com um agendamento.

Com base nos resultados dessa amostragem, o Kaspersky Security Center Cloud Console atualiza a lista de dispositivos não atribuídos. Você também pode configurar regras para dispositivos recém localizados serem movidos automaticamente para grupos de administração.

O Kaspersky Security Center Cloud Console usa os seguintes métodos de amostragem da rede:

- *Amostragem da faixa IP*. O Kaspersky Security Center Cloud Console faz a amostragem das faixas IP especificadas usando pacotes Internet Control Message Protocol (ICMP) e compila um conjunto de dados completo nos dispositivos dentro dessas faixas IP.

- *Amostragem da rede do Windows*. Você pode executar uma das duas amostragens da rede do Windows: rápida ou completa. Durante uma amostragem rápida, o Kaspersky Security Center Cloud Console somente recupera a informação da lista dos nomes de NetBIOS dos dispositivos em todos os domínios da rede e grupos de trabalho. Durante a amostragem completa, as seguintes informações são solicitadas de cada dispositivo: sistema operacional (SO), endereço IP, nome DNS e nome NetBIOS.

- *Sondagem dos controladores de domínio*. As informações sobre a estrutura da unidade do Active Directory e sobre os nomes DNS dos dispositivos dos grupos do Active Directory são registradas no banco de dados do Kaspersky Security Center Cloud Console.

Os resultados da sondagem são exibidos na seção **Descoberta e implementação → Descoberta** separadamente para os métodos de *Sondagem de rede do Windows* e de *Sondagem de controladores de domínio*.

Os resultados da sondagem para o método de *sondagem do intervalo IP* são exibidos na seção **Descoberta e implementação → Dispositivos não atribuídos**.

Um dispositivo pode ser mostrado em mais de uma área de detecção. Se um dispositivo for detectado no domínio HQ e seu endereço for 192.168.0.1, o dispositivo aparecerá na seção **Domínios do Windows** e na seção **Dispositivos não atribuídos**. Você pode modificar as configurações de amostragem da rede para cada método de amostragem. Por exemplo, é possível modificar o agendamento de amostragem ou definir se deve amostrar toda a floresta do Active Directory ou apenas um domínio específico.

Sondagem da rede do Windows

Sobre a sondagem de rede do Windows

Durante uma sondagem rápida, o Servidor de Administração somente recupera a informação da lista dos nomes de NetBIOS dos dispositivos em todos os domínios da rede e grupos de trabalho. Durante uma sondagem completa, as seguintes informações são solicitadas de cada dispositivo cliente:

- Nome de sistema operacional
- Endereço IP
- Nome DNS
- Nome NetBIOS

As sondagens rápida e completa requerem o seguinte:

- As portas UDP 137/138, TCP 139 devem estar disponíveis na rede.
- O serviço Microsoft Computer Browser deve ser usado, e o navegador principal do computador deve estar ativado no ponto de distribuição.
- O serviço Microsoft Computer Browser deve ser usado, e o navegador principal do computador deve estar ativado nos dispositivos cliente:
  - Em pelo menos um dispositivo, se o número de dispositivos em rede não exceder 32.
  - Em pelo menos um dispositivo para cada 32 dispositivos em rede.

A sondagem completa poderá ser executada apenas se a sondagem rápida tiver sido executada pelo menos uma vez.

Visualização e alteração das configurações para a sondagem da rede Windows

Para modificar as propriedades da sondagem da rede do Windows:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.
3. Clique no nome do ponto de distribuição que você deseja usar para efetuar a sondagem da rede.

   A janela Propriedades do ponto de distribuição é aberta.

4. Selecione a seção **Sondagem dos domínios do Windows**.
5. Ative ou desative a sondagem de rede do Windows usando o botão de alternar **Ativar sondagem da rede**.

6. Configure o agendamento para a sondagem rápida e a sondagem completa.

7. Clique no botão **OK**.

As propriedades são salvas e aplicadas a todos os domínios e grupos de trabalho do Windows descobertos.

Sondagem do controlador de domínio

O Kaspersky Security Center Cloud Console é compatível com a sondagem de um controlador de domínio do Microsoft Active Directory e um controlador de domínio Samba. Para um controlador de domínio Samba, o Samba 4 é usado como um controlador de domínio do Active Directory.

Ao fazer a sondagem de um controlador de domínio, o ponto de distribuição recupera as informações sobre a estrutura do domínio, contas de usuário, grupos de segurança e nomes DNS dos dispositivos incluídos no domínio. A sondagem do controlador de domínio é executada de acordo com um agendamento definido por você.

Pré-requisitos

Antes de fazer a sondagem de um controlador de domínio, verifique e confirme se os seguintes protocolos estão ativados:

- Simple Authentication and Security Layer (SASL)
- Lightweight Directory Access Protocol (LDAP)

Verifique e confirme se as seguintes portas estão disponíveis no dispositivo controlador de domínio:

- 389 para SASL
- 636 para TLS

A sondagem do controlador de domínio com o uso de um ponto de distribuição

Também é possível sondar um controlador de domínio com o uso de um ponto de distribuição. Um dispositivo gerenciado baseado em Windows ou Linux pode atuar como um ponto de distribuição.

Para um ponto de distribuição do Linux, há suporte para a sondagem de um controlador de domínio do Microsoft Active Directory e de um controlador de domínio Samba.
Para um ponto de distribuição do Windows, apenas a sondagem de um controlador de domínio do Microsoft Active Directory é compatível.
A sondagem com um ponto de distribuição Mac não é compatível.

Para configurar a sondagem do controlador de domínio com o uso do ponto de distribuição:

1. Abra as propriedades do ponto de distribuição.

2. Selecione a seção **Sondagem do controlador de domínio**.

3. Selecione a opção **Ativar sondagem do controlador de domínio**.

4. Selecione o controlador de domínio que deseja sondar.

   Caso queira usar um ponto de distribuição do Linux, na seção **Sondar domínios especificados**, clique em **Adicionar** e especifique o endereço e as credenciais de usuário do controlador de domínio.

   Se você usar um ponto de distribuição do Windows, poderá selecionar uma das seguintes opções:

   - **Sondar domínio atual**
   - **Sondar toda a floresta de domínios**
   - **Sondar domínios especificados**

5. Clique no botão **Definir agendamento da sondagem** para especificar as opções de agendamento de sondagem, caso seja necessário.

   A sondagem é iniciada de acordo com o agendamento especificado apenas. O início manual da sondagem não está disponível.

Após a conclusão da sondagem, a estrutura do domínio será exibida na seção **Controladores de domínio**.

Se você tiver configurado e ativado as regras para migrar dispositivos, os dispositivos recentemente descobertos estarão automaticamente incluídos no grupo **Dispositivos gerenciados**. Se nenhuma regra de movimento tiver sido ativada, os dispositivos recentemente descobertos serão automaticamente incluídos no grupo **Dispositivos não atribuídos**.

As contas de usuário descobertas podem ser usadas para autenticação do domínio no Kaspersky Security Center Cloud Console.

Visualização dos resultados da pesquisa do controlador de domínio

Para visualizar os resultados da sondagem do controlador de domínio:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Controladores de domínio**.

   A lista de unidades organizacionais descobertas é exibida.

2. Selecione uma unidade organizacional e clique no botão **Dispositivos**.

   A lista de dispositivos na unidade organizacional é exibida.

Você pode pesquisar a lista e filtrar os resultados.

Sondagem do conjunto de IPs

O Kaspersky Security Center Cloud Console tenta executar a resolução de nome inversa para cada endereço do intervalo especificado para um nome de DNS usando solicitações de DNS padrão. Se essa operação tiver sucesso, o servidor enviará uma `ICMP ECHO REQUEST` (da mesma forma que o comando ping) ao nome recebido. Se o dispositivo responder, as informações sobre ele serão adicionadas ao banco de dados do Kaspersky Security Center Cloud Console. A resolução de nome inversa é necessária para excluir os dispositivos de rede que podem ter um endereço IP, mas não são computadores, por exemplo, impressoras em rede ou roteadores.

Esse método de sondagem depende de um serviço de DNS local corretamente configurado. Ele deve ter uma zona de pesquisa inversa. Se essa zona não estiver configurada, a sondagem de sub-rede IP não produzirá nenhum resultado. Nas redes em que o Active Directory é usado, tal zona é mantida automaticamente. Mas nessas redes, a sondagem de sub-rede de IP não fornece mais informações do que a sondagem do Active Directory. Além disso, os administradores de pequenas redes muitas vezes não configuram a zona de pesquisa inversa porque não ela é necessária para o funcionamento de muitos serviços de rede. Por esses motivos, a sondagem de sub-rede de IP é desativada por padrão.

Inicialmente, o Kaspersky Security Center Cloud Console obtém intervalos de IPs para a sondagem da rede em configurações do dispositivo de ponto de distribuição usado para a sondagem da rede. Se o endereço de dispositivo for 192.168.0.1 e a máscara de subrede for 255.255.255.0, o Kaspersky Security Center Cloud Console incluirá a rede 192.168.0.0/24 na lista do endereço de sondagem automaticamente. O Kaspersky Security Center Cloud Console faz a sondagem de todos os endereços de 192.168.0.1 a 192.168.0.254.

Não se recomenda usar a amostragem de conjuntos de IPs se você usar a amostragem de rede do Windows e/ou a amostragem do Active Directory.

Visualização e modificação de configurações para amostragem de faixas IP

Para visualizar e modificar as propriedades para amostragem de faixas IP:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Clique no nome do ponto de distribuição que você deseja usar para efetuar a sondagem da rede.

   A janela Propriedades do ponto de distribuição é aberta.

4. Selecione a seção **Sondagem dos intervalos de IP**.

5. Ative ou desative a sondagem de IP usando o botão de alternar **Ativar sondagem de intervalos**.

6. Configure o agendamento da sondagem. Por padrão, a amostragem de IP é executada a cada 420 minutos (sete horas).

7. Se necessário, adicione ou modifique os intervalos de IP para sondagem.

   Ao especificar o intervalo de amostragem, assegure-se de que essa configuração não exceda o valor do parâmetro de duração do endereço IP. Se um endereço IP não for verificado por sondagem durante a duração do endereço IP, esse endereço IP será automaticamente removido dos resultados da sondagem. Por padrão, a duração dos resultados da sondagem é de 24 horas, pois os endereços IP dinâmicos (atribuídos com o uso de Dynamic Host Configuration Protocol (DHCP)) mudam a cada 24 horas.

8. Clique no botão **OK**.

As propriedades são salvas e aplicadas a todos os conjuntos de IPs.

Configuração de um controlador de domínio Samba

O Kaspersky Security Center Cloud Console oferece suporte a um controlador de domínio Linux executado apenas no Samba 4.

Um controlador de domínio Samba é compatível com as mesmas extensões de esquema que um controlador de domínio Microsoft Active Directory. É possível ativar a compatibilidade total de um controlador de domínio Samba com um controlador de domínio Microsoft Active Directory usando a extensão de esquema Samba 4. Essa é uma ação opcional.

Recomendamos ativar a compatibilidade total de um controlador de domínio Samba com um controlador de domínio Microsoft Active Directory. Isso garantirá a interação correta entre o Kaspersky Security Center Cloud Console e o controlador de domínio Samba.

Para ativar a compatibilidade total de um controlador de domínio Samba com um controlador de domínio Microsoft Active Directory:

1. Execute o seguinte comando para usar a extensão de esquema RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Ative a atualização do esquema em um controlador de domínio Samba. Para fazer isso, adicione as seguintes linhas ao arquivo /etc/samba/smb.conf:

   ```
   dsdb:schema update allowed = true
   ```

   Caso a atualização do esquema seja concluída com um erro, será necessário executar uma restauração completa do controlador de domínio que atua como controlador principal do esquema.

Para fazer a sondagem de um controlador de domínio Samba corretamente, especifique o `nome Netbios` e os parâmetros do `grupo de trabalho` no arquivo /etc/samba/smb.conf.

Adição e modificação de um conjunto de IPs

Inicialmente, o Kaspersky Security Center Cloud Console obtém intervalos de IPs para a sondagem da rede em configurações do dispositivo de ponto de distribuição usado para a sondagem da rede. Se o endereço de dispositivo for 192.168.0.1 e a máscara de subrede for 255.255.255.0, o Kaspersky Security Center Cloud Console incluirá a rede 192.168.0.0/24 na lista do endereço de sondagem automaticamente. O Kaspersky Security Center Cloud Console faz a sondagem de todos os endereços de 192.168.0.1 a 192.168.0.254. Você pode modificar os conjuntos de IPs definidos automaticamente ou adicionar conjuntos de IPs personalizados.

Para adicionar um novo conjunto de IPs:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Clique no nome do ponto de distribuição que você deseja usar para efetuar a sondagem da rede.

   A janela Propriedades do ponto de distribuição é aberta.

4. Selecione a seção **Sondagem dos intervalos de IP**.

5. Para adicionar um novo conjunto de IPs, clique no botão **Adicionar**.

6. Na janela que for aberta, especifique as seguintes configurações:

- **Nome**

  Um nome do conjunto de IPs. Você pode especificar o próprio conjunto de IPs como o nome, por exemplo, "192.168.0.0/24".

- **Intervalo de IP ou endereço e máscara de sub-rede**

  Defina o conjunto de IPs especificando os endereços IP inicial e final ou o endereço de sub-rede e a máscara de sub-rede. Você pode adicionar quantas sub-redes precisar. Não é permitido que os conjuntos de IPs se sobreponham, mas as sub-redes não nomeadas dentro de um conjunto de IPs não têm tais restrições.

- **Duração do endereço IP (horas)**

  Ao especificar esse parâmetro, verifique se ele excede o conjunto de intervalos de sondagem no agendamento de sondagem. Se um endereço IP não for verificado por sondagem durante a duração do endereço IP, esse endereço IP será automaticamente removido dos resultados da sondagem. Por padrão, a duração dos resultados da sondagem é de 24 horas, pois os endereços IP dinâmicos (atribuídos com o uso de Dynamic Host Configuration Protocol (DHCP)) mudam a cada 24 horas.

7. Clique no botão **OK**.

O novo conjunto de IPs é adicionado à lista de conjuntos de IPs.

Quando a sondagem é concluída, será possível visualizar a lista de dispositivos descobertos usando o botão **Dispositivos**. Por padrão, a duração dos resultados da sondagem é de 24 horas e é igual à configuração de duração do endereço IP.

Ajuste de pontos de distribuição e gateways de conexão

Uma estrutura de grupos de administração no Kaspersky Security Center Cloud Console executa as seguintes funções:

- Define o escopo das políticas

  Há um modo alternativo para aplicar configurações relevantes nos dispositivos, usando *perfis de política*. Neste caso, o escopo das políticas é definido com tags, localizações de dispositivos nas unidades organizacionais do Active Directory, associação nos grupo de segurança do Active Directory e etc.

- Define o escopo da tarefas de grupo

  Há uma abordagem para definir o escopo da tarefas de grupo que não tem base em uma hierarquia de grupos de administração: uso de tarefas para seleções de dispositivos e tarefas para dispositivos específicos.

- Define os direitos de acesso aos dispositivos e Servidores de Administração secundários

- Atribui os pontos de distribuição

Ao criar a estrutura de grupos de administração, você deve levar em conta a topologia da rede da organização para a atribuição ótima de pontos de distribuição. A distribuição ideal dos pontos de distribuição permite poupar tráfego na rede da organização.

Dependendo do esquema da organização e da topologia da rede, as seguintes configurações padrão podem ser aplicadas à estrutura de grupos de administração:

- Escritório único
- Múltiplos pequenos escritórios remotos

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Calcular o número e a configuração de pontos de distribuição

Quanto mais dispositivos cliente uma rede contiver, mais pontos de distribuição ela exigirá. Use as tabelas abaixo para calcular o número de pontos de distribuição necessários para a sua rede.

Certifique-se de que os dispositivos que você pretende usar como pontos de distribuição tenham um volume suficiente de espaço livre em disco, não sejam desligados regularmente e estejam com o modo Suspenso desativado.

Número de pontos de distribuição exclusivamente atribuídos em uma rede que contém um segmento de rede único, com base no número de dispositivos na rede

Número de dispositivos cliente em o segmento da rede	Número de pontos de distribuição
Menos de 300	0 (Não atribuir os pontos de distribuição)
Mais de 300	Aceitável: (N/10.000 + 1), recomendado: (N/5000 + 2), onde N é o número de dispositivos em rede

Número de pontos de distribuição exclusivamente atribuídos em uma rede que contém vários segmentos de rede, com base no número de dispositivos na rede

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
Menos de 10	0 (Não atribuir os pontos de distribuição)
10... 100	1
Mais de 100	Aceitável: (N/10.000 + 1), recomendado: (N/5000 + 2), onde N é o número de dispositivos em rede

Usar dispositivos cliente padrão (estações de trabalho) como pontos de distribuição

Se você planejar usar dispositivos cliente padrão (isto é, estações de trabalho) como pontos de distribuição, recomendamos atribuir pontos de distribuição, como mostrado nas tabelas abaixo, para evitar a carga excessiva dos canais de comunicação e do Servidor de Administração:

O número de estações de trabalho que funcionam como pontos de distribuição em uma rede que contém um segmento de rede único, com base no número de dispositivos na rede

Número de dispositivos cliente em o segmento da rede	Número de pontos de distribuição
Menos de 300	0 (Não atribuir os pontos de distribuição)
Mais de 300	(N/300 + 1), onde N é o número de dispositivos em rede; deve haver pelo menos 3 pontos de distribuição

O número de estações de trabalho que funcionam como pontos de distribuição em uma rede que contém vários segmentos de rede, com base no número de dispositivos na rede

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
Menos de 10	0 (Não atribuir os pontos de distribuição)
10... 30	1
31... 300	2
Mais de 300	(N/300 + 1), onde N é o número de dispositivos em rede; deve haver pelo menos 3 pontos de distribuição

Se um ponto de distribuição não estiver disponível, atualize os bancos de dados, módulos de software e aplicativos da Kaspersky manualmente ou diretamente a partir dos servidores de atualização da Kaspersky.

Configuração padrão de pontos de distribuição: escritório único

Em uma configuração de "escritório único" padrão, todos os dispositivos estão dentro da rede da organização, portanto eles podem se "ver" mutuamente. A rede da organização pode consistir em algumas partes separadas (redes ou segmentos de rede) vinculadas por canais estreitos.

Os seguintes métodos de criar a estrutura de grupos de administração são possíveis:

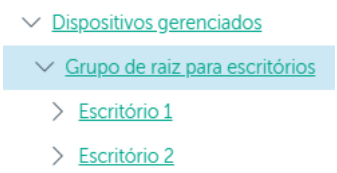
- Criar uma estrutura de grupos de administração levando em consideração a topologia da rede. A estrutura de grupos de administração pode não refletir a topologia da rede com uma precisão absoluta. Uma coincidência entre as partes separadas da rede e determinados grupos de administração seria suficiente.

- Criar uma estrutura de grupos de administração não levando em consideração a topologia da rede. Neste caso, você atribuir um ou diversos dispositivos para atuar como pontos de distribuição de um grupo de administração raiz em cada uma das partes separadas da rede, por exemplo, para o grupo **Dispositivos gerenciados**. Todos os pontos de distribuição estarão no mesmo nível e apresentarão a mesma expansão de escopo para todos os dispositivos na rede da organização. Nesse caso, cada Agente de Rede se conectará ao ponto de distribuição que tenha a rota mais curta. A rota para um ponto de distribuição pode ser traçada com o utilitário tracert.

Configuração padrão de pontos de distribuição: múltiplos pequenos escritórios remotos

Esta configuração padrão proporciona uma série de pequenos escritórios remotos, que podem se comunicar com a sede através da Internet. Cada escritório remoto é localizado além da NAT, ou seja, a conexão de um escritório remoto ao outro não é possível porque os escritórios estão isolados entre si.

A configuração deve ser refletida na estrutura de grupos de administração: um grupo de administração separado deve ser criado para cada escritório remoto (grupos **Escritório 1** e **Escritório 2** na figura abaixo).



Os escritórios remotos estão incluídos na estrutura do grupo de administração

Um ou vários pontos de distribuição devem ser atribuídos à cada grupo de administração que corresponda a um escritório. Os pontos de distribuição devem ser dispositivos nos escritórios remotos que têm espaço livre suficiente em disco. Os dispositivos implementados no grupo **Escritório 1**, por exemplo, acessarão os pontos de distribuição atribuídos ao grupo de administração **Escritório 1**.

Se alguns usuários se moverem entre escritórios fisicamente, com os seus computadores portáteis, você deve selecionar dois ou mais dispositivos (além dos pontos de distribuição existentes) em cada escritório remoto e atribui-los para atuar como pontos de distribuição para um grupo de administração de nível superior (**Grupo de raiz para escritórios** na figura acima).

Exemplo: Um computador portátil é implementado no grupo de administração **Escritório 1** e então é movido fisicamente para o escritório que corresponde ao grupo de administração **Escritório 2**. Após o computador portátil ter sido movido, o Agente de Rede tenta acessar os pontos de distribuição atribuídos ao grupo **Escritório 1**, mas aqueles pontos de distribuição estão indisponíveis. Então, O Agente de Rede começa a tentar acessar os pontos de distribuição que foram atribuídos ao **Grupo de raiz para escritórios**. Como os escritórios remotos estão isolados entre si, as tentativas de acessar os pontos de distribuição atribuídos ao grupo de administração **Grupo raiz para escritórios** somente terão êxito quando o Agente de Rede tentar acessar os pontos de distribuição no grupo **Escritório 2**. Ou seja, o computador portátil permanecerá no grupo de administração que corresponde ao escritório inicial, mas o computador portátil usará o ponto de distribuição do escritório onde estiver fisicamente localizado no momento.

Atribuir os pontos de distribuição manualmente

O Kaspersky Security Center Cloud Console permite atribuir dispositivos manualmente para atuarem como pontos de distribuição. Recomendamos que você calcule o número e a configuração de pontos de distribuição necessários para a rede.

Os dispositivos de ponto de distribuição executando macOS não podem baixar atualizações dos servidores de atualização da Kaspersky.

Se um ou mais dispositivos executando macOS estiverem dentro do escopo da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a tarefa será concluída com o status *Falha*, mesmo se for concluída com êxito em todos os dispositivos Windows.

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Para atribuir manualmente os dispositivos para agir como ponto de distribuição:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Clique no botão **Atribuir**.

4. Selecione o dispositivo que você quer atribuir como ponto de distribuição.

   Ao selecionar um dispositivo, tenha em mente os recursos da operação de pontos de distribuição e os requisitos definidos para o dispositivo que age como ponto de distribuição.

5. Selecione o grupo de administração que você quer incluir no escopo do ponto de distribuição selecionado.

6. Clique no botão **Adicionar**.

O pontos de distribuição que você adicionou será exibido na lista de pontos de distribuição na seção **Pontos de distribuição**.

7. Selecione o ponto de distribuição recém adicionado na lista para abrir sua janela de propriedades.

8. Configure o ponto de distribuição na janela de propriedades:

- A seção **Geral** contém as configurações de interação entre o ponto de distribuição e os dispositivos cliente:

  - **Porta SSL**

    O número da porta SSL para a conexão criptografada entre dispositivos cliente e o ponto de distribuição usando SSL.

    Por padrão, a porta 13000 é usada.

  - **Usar multicast**

    Se esta opção estiver ativada, o IP multicasting será usado para distribuição automática de pacotes de instalação para dispositivos cliente dentro do grupo.

    O multicast de IP diminui o tempo necessário para instalar um aplicativo de um pacote de instalação em um grupo de dispositivos cliente, mas aumenta o tempo de instalação quando você instala um aplicativo em um único dispositivo cliente.

  - **Endereço IP multicast**

    O endereço IP que será usado para multicasting. Você pode definir um endereço IP no conjunto de 224.0.0.0 – 239.255.255.255

    Por padrão, o Kaspersky Security Center Cloud Console atribui automaticamente um endereço IP multicast exclusivo dentro do conjunto especificado.

  - **Número da porta de IP multicast**

    Número da porta para multicasting de IP.

    Por padrão, o número de porta é 15001. Se o dispositivo com o Servidor de Administração instalado for especificado como o ponto de distribuição, por padrão a porta 13001 é usada para conexão SSL.

  - **Implementar atualizações**

    As atualizações são distribuídas para dispositivos gerenciados a partir das seguintes fontes:

    - Este ponto de distribuição, caso esta opção esteja ativada.
    - Outros pontos de distribuição, o Servidor de Administração ou os servidores de atualização da Kaspersky, caso esta opção esteja desativada.

    Caso utilize os pontos de distribuição para implantar atualizações, será possível economizar tráfego, pois o número de downloads será reduzido. Além disso, é possível aliviar a carga no Servidor de Administração e realocar a carga entre os pontos de distribuição. É possível calcular o número de pontos de distribuição para a rede e otimizar o tráfego e a carga.

    Caso essa opção seja desativada, o número de downloads de atualização e a carga no Servidor de Administração podem aumentar. Por padrão, esta opção está ativada.

- **Implementar pacotes de instalação**

  Os pacotes de instalação são distribuídos para dispositivos gerenciados a partir das seguintes fontes:

  - Este ponto de distribuição, caso esta opção esteja ativada.
  - Outros pontos de distribuição, o Servidor de Administração ou os servidores de atualização da Kaspersky, caso esta opção esteja desativada.

  Se você usar pontos de distribuição para implementar pacotes de instalação, poderá economizar tráfego porque reduz o número de downloads. Além disso, é possível aliviar a carga no Servidor de Administração e realocar a carga entre os pontos de distribuição. É possível calcular o número de pontos de distribuição para a rede e otimizar o tráfego e a carga.

  Caso essa opção seja desativada, o número de downloads de pacotes de instalação e a carga no Servidor de Administração podem aumentar. Por padrão, esta opção está ativada.

- **Executar servidor push**

  No Kaspersky Security Center Cloud Console, um ponto de distribuição pode funcionar como um servidor push para dispositivos baseados em Windows e Linux gerenciados pelo Agente de Rede. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Caso tenha vários pontos de distribuição atribuídos ao mesmo grupo de administração, será possível ativar um servidor push em cada um dos pontos de distribuição. Nesse caso, o Servidor de Administração equilibra a carga entre os pontos de distribuição.

- **Porta do servidor push**

  O número da porta para o servidor push. É possível especificar o número de qualquer porta livre.

- Na seção **Escopo**, especifique o escopo ao qual o ponto de distribuição distribuirá as atualizações (grupos de administração e/ou uma localização da rede).

  Somente os dispositivos sendo executados no sistema operacional Windows podem determinar a sua localização na rede. A localização da rede não pode ser determinada para dispositivos que executam outros sistemas operacionais.

- Na seção **Proxy da KSN**, você pode configurar o aplicativo para usar o ponto de distribuição para encaminhar solicitações do KSN a partir dos dispositivos gerenciados:

  Ativar o proxy da KSN no lado do ponto de distribuição

O serviço Proxy da KSN é executado no dispositivo que é usado como um ponto de distribuição. Use este recurso para redistribuir e otimizar o tráfego na rede.

Esse recurso não tem suporte de dispositivos de ponto de distribuição executando Linux ou macOS.

O ponto de distribuição envia as estatísticas da KSN, que são listadas na Declaração da Kaspersky Security Network, à Kaspersky. Por padrão, a Declaração da KSN está localizada em %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Por padrão, esta opção está desativada. A ativação desta opção somente tem efeito se a opção **Concordo em usar a Kaspersky Security Network** estiver ativada na janela de propriedades do Servidor de Administração.

É possível atribuir um nó de um cluster ativo-passivo a um ponto de distribuição e habilitar o servidor proxy da KSN nesse nó.

- Configure a amostragem de domínios do Windows, Active Directory e faixas IP pelo ponto de distribuição:
  - Sondagem dos domínios do Windows

    Você pode ativar a descoberta de dispositivos para domínios do Windows e definir o agendamento para a localização.

  - Active Directory

    Você pode ativar a sondagem da rede para o Active Directory e definir o agendamento da sondagem.

    Se você usar um ponto de distribuição do Windows, poderá selecionar uma das seguintes opções:

    - **Sondar o domínio atual do Active Directory**.
    - **Sondar a floresta de domínios do Active Directory**.
    - **Criar sondagem apenas de domínios selecionados do Active Directory**. Se você selecionar esta opção, adicione um ou mais domínios do Active Directory à lista.

    Se você usar um ponto de distribuição do Linux com o Agente de Rede versão 15 instalado, poderá sondar somente domínios do Active Directory para os quais o endereço e as credenciais do usuário foram especificados. A sondagem do domínio atual do Active Directory e da floresta de domínios do Active Directory não está disponível.

  - Sondagem dos intervalos de IP

Você pode ativar a descoberta de dispositivos para conjuntos IPv4 e redes IPv6.

Ao ativar a opção **Ativar sondagem de conjuntos**, você poderá adicionar conjuntos verificados e definir seu agendamento. Você pode adicionar conjuntos de IPs à lista de conjuntos verificados.

Ao ativar a opção **Usar Zeroconf para sondar redes IPv6**, o ponto de distribuição sonda automaticamente a rede IPv6 usando rede zero configuração (também referida como *Zeroconf*). Nesse caso, os conjuntos IP especificados são ignorados, pois o ponto de distribuição sonda toda a rede. A opção **Usar Zeroconf para sondar redes IPv6** estará disponível caso o ponto de distribuição execute Linux. Para usar a sondagem do Zeroconf IPv6, é necessário instalar o utilitário avahi-browse no ponto de distribuição.

- Na seção **Avançado**, especifique a pasta que o ponto de distribuição deve usar para armazenar os dados distribuídos.
  - Usar pasta padrão

    Se você selecionar esta opção, o aplicativo usa a pasta de Instalação do Agente de Rede no ponto de distribuição.

  - Usar pasta especificada

    Se selecionar esta opção, você pode, no campo abaixo, especificar o caminho até a pasta. Pode ser uma pasta local no ponto de distribuição ou pode ser uma pasta em qualquer dispositivo na rede corporativa.

    A conta do usuário usada no ponto de distribuição para executar o Agente de Rede deve ter acesso de leitura/gravação à pasta especificada.

9. Clique no botão **OK**.

Os dispositivos selecionados agirão como pontos de distribuição.

Modificar a lista de pontos de distribuição para um grupo de administração

Você pode visualizar a lista de pontos de distribuição atribuídos a um grupo de administração específico e modificá-la adicionando ou removendo pontos de distribuição.

Para visualizar e modificar a lista de pontos de distribuição atribuídos a um grupo de administração:

1. No menu principal, vá para **Ativos (dispositivos)** → **Grupos**.
2. Na estrutura de grupos de administração, selecione o grupo de administração para o qual você deseja visualizar os pontos de distribuição atribuídos.
3. Clique na guia **Pontos de distribuição**.
4. Adicione novos pontos de distribuição ao grupo de administração usando o botão **Atribuir** ou remova os pontos de distribuição atribuídos usando o botão **Desatribuir**.

Dependendo das suas modificações, os novos pontos de distribuição serão adicionados à lista ou os pontos de distribuição existentes serão removidos da lista.

Usando um ponto de distribuição como um servidor push

No Kaspersky Security Center Cloud Console, um ponto de distribuição pode funcionar como um servidor push para dispositivos baseados em Windows e Linux gerenciados pelo Agente de Rede. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Caso tenha vários pontos de distribuição atribuídos ao mesmo grupo de administração, será possível ativar um servidor push em cada um dos pontos de distribuição. Nesse caso, o Servidor de Administração equilibra a carga entre os pontos de distribuição.

É possível usar pontos de distribuição como servidores push para garantir conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração. A conectividade contínua é necessária para algumas operações, como executar e interromper tarefas locais, receber estatísticas de um aplicativo gerenciado ou criar um túnel. Caso use um ponto de distribuição como servidor push, não será necessário enviar pacotes para a porta UDP do Agente de Rede.

Para usar um ponto de distribuição como servidor push:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Clique no ponto de distribuição que deseja usar como servidor push.

4. Na lista de propriedades do ponto de distribuição selecionado, vá para a seção **Geral** e ative a opção **Executar servidor push**.

   O campo de entrada **Porta do servidor push** fica disponível.

5. No campo de entrada da **Porta do servidor push**, especifique a porta no ponto de distribuição que os dispositivos cliente usarão para conexão. Por padrão, a porta 13295 é usada.

   > Para estabelecer uma conexão entre o ponto de distribuição que atua como servidor push e um dispositivo gerenciado, é necessário adicionar manualmente a porta do servidor push especificada na lista de exclusão do firewall do Microsoft Windows.

6. Clique em **OK** para sair da janela de propriedades do ponto de distribuição e, a seguir, clique em **Salvar** para aplicar as alterações.

   Depois de ativar a opção **Executar servidor push**, a opção **Não desconectar do Servidor de Administração** é ativada automaticamente no ponto de distribuição que atua como servidor push. Essa opção fornece uma conexão precoce entre o Agente de Rede e o Servidor de Administração.

7. Abra a janela de Configurações de política do Agente de Rede.

8. Vá para **Conectividade** → **Rede** e ative a opção **Usar o ponto de distribuição para forçar a conexão ao Servidor de Administração**. Feche o cadeado para essa opção.

9. Na subseção **Rede**, também é possível desativar a opção **Usar porta UDP**. O servidor push configurado fornecerá conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração em vez de enviar pacotes pela porta UDP.

10. Clique no botão **OK** para sair da janela.

O ponto de distribuição começará a atuar como um servidor push. Ele pode agora enviar notificações push para dispositivos clientes.

Uso da opção "Não desconectar do Servidor de Administração" para fornecer conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração

Caso os servidores push não sejam usados, o Kaspersky Security Center Cloud Console não fornecerá conectividade contínua entre dispositivos gerenciados e o Servidor de Administração. Os Agentes de Rede em dispositivos gerenciados periodicamente estabelecem conexões e sincronizam com o Servidor de Administração. O intervalo entre as sessões de sincronização é definido em uma política do Agente de Rede. Caso seja necessária uma sincronização antecipada, o Servidor de Administração (ou um ponto de distribuição, se estiver em uso) enviará um pacote de rede assinado por uma rede IPv4 ou IPv6 para a porta UDP do Agente de Rede. Por padrão, o número de porta é 15000. Caso nenhuma conexão via UDP seja possível entre o Servidor de Administração e um dispositivo gerenciado por qualquer motivo, a sincronização será executada na próxima conexão regular entre o agente de rede e o Servidor de Administração dentro do intervalo de sincronização.

Algumas operações não podem ser executadas sem uma conexão antecipada entre o agente de rede e o Servidor de Administração, como executar e interromper tarefas locais, receber estatísticas de um aplicativo gerenciado ou criar um túnel. Para resolver esse problema, caso os servidores push não estejam sendo usados, será possível usar a opção **Não desconectar do Servidor de Administração** para se certificar de que haja conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração.

Para fornecer conexão contínua entre um dispositivo gerenciado e o Servidor de Administração:

1. Execute uma das seguintes ações:

   - Caso o dispositivo gerenciado acesse o Servidor de Administração diretamente (ou seja, não por meio de um ponto de distribuição):

     a. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.

     b. Clique no nome do dispositivo com o qual deseja fornecer conectividade contínua.

     A janela de propriedades do dispositivo gerenciado é aberta.

   - Caso o dispositivo gerenciado acesse o Servidor de Administração por meio de um ponto de distribuição em execução no modo gateway, não diretamente:

     a. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

     A janela Propriedades do Servidor de Administração é aberta.

     b. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

     c. Na lista de pontos de distribuição, clique no nome do ponto de distribuição requerido.

     A janela de propriedades do ponto de distribuição selecionado é aberta.

2. Na seção **Geral** da janela de propriedades aberta, selecione a opção **Não desconectar do Servidor de Administração**.

A conectividade contínua é estabelecida entre o dispositivo gerenciado e o Servidor de Administração.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Criação de grupos de administração

Inicialmente, a hierarquia de grupos de administração contém o único grupo de administração denominado **Dispositivos gerenciados**. Ao criar uma hierarquia de grupos de administração, será possível adicionar dispositivos e máquinas virtuais ao grupo e subgrupo **Dispositivos gerenciados**. Para cada grupo de administração, a janela de propriedades contém informações sobre políticas, tarefas e dispositivos relacionados ao grupo.

Para criar um grupo de administração:

1. No menu principal, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Selecione a caixa de seleção ao lado do grupo de administração para o qual você deseja criar um novo subgrupo.
3. Clique no botão **Adicionar**.
4. Digite um nome para o novo grupo de administração.
5. Clique no botão **Adicionar**.

Um novo grupo de administração com o nome especificado aparece na hierarquia do grupo de administração.

O aplicativo permite criar uma hierarquia dos grupos de administração com base na estrutura do Active Directory ou na estrutura de domínio da rede. Você também pode criar uma estrutura de grupos a partir de um arquivo de texto.

Para criar a estrutura de grupos de administração:

1. No menu principal, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Clique no botão **Importar**.

O Assistente de Nova Estrutura de Grupos de Administração é iniciado. Siga as instruções do Assistente.

Criar regras para mover dispositivos

É possível configurar as regras de migração de dispositivos, ou seja, as regras que alocam automaticamente os dispositivos para grupos de administração.

Para criar uma regra para mover dispositivos:

1. No menu principal, vá para **Ativos (dispositivos)** → **Regras de migração**.
2. Clique em **Adicionar**.
3. Na janela exibida, especifique as seguintes informações na guia **Geral**:

- **Nome da regra**

  Digite um nome para a nova regra.

  Se estiver copiando uma regra, a nova regra adquirirá o mesmo nome da regra de origem, mas um índice no formato () será adicionado ao nome, por exemplo: (1).

- **Grupo de administração**

  Selecione o grupo de administração para o qual os dispositivos devem ser movidos automaticamente.

- **Regra ativa**

  Se esta opção estiver ativada, a regra será ativada e começará a funcionar após ser salva.

  Se esta opção estiver desativada, a regra será criada, mas não ativada. Ela não funcionará até que você ative esta opção.

- **Somente migrar os dispositivos que não pertencem a um grupo de administração**

  Se esta opção estiver ativada, somente os dispositivos não atribuídos serão movidos para o grupo selecionado.

  Se esta opção estiver desativada, os dispositivos que já pertencem a outros grupos de administração, bem como os dispositivos não atribuídos, serão movidos para o grupo selecionado.

- **Aplicar regra**

  Você pode selecionar uma das seguintes opções:

  - **Executar uma vez para cada dispositivo**

    A regra é aplicada uma vez para cada dispositivo que atenda aos critérios.

  - **Executar uma vez para cada dispositivo e depois em cada reinstalação do Agente de Rede**

    A regra é aplicada uma vez para cada dispositivo que atende aos critérios e apenas quando o Agente de Rede é reinstalado nesses dispositivos.

  - **Aplicar regra continuamente**

    A regra é aplicada de acordo com o agendamento que o Servidor de Administração configura automaticamente (normalmente a cada várias horas).

4. Na guia **Condições da regra**, especifique pelo menos um critério pelo qual os dispositivos são movidos para um grupo de administração.

5. Clique em **Salvar**.

A regra de movimentação é criada. Ela é exibida na lista de regras de movimento.

Quanto mais elevada a posição na lista, maior a prioridade da regra. Para aumentar ou diminuir a prioridade de uma regra em movimento, mova a regra para cima ou para baixo na lista, respectivamente, usando o mouse.

Se os atributos do dispositivo atenderem as condições de múltiplas regras, o dispositivo é movido para o grupo alvo da regra com a prioridade mais alta (ou seja, ele tem a classificação mais alta na lista de regras).

Copiar as regras para mover dispositivos

Você poderá copiar regras de movimento, por exemplo, se quiser ter várias regras idênticas para grupos de administração de destino diferentes.

Para copiar uma regra de movimentação existente:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Ativos (dispositivos)** → **Regras de migração**.
   - No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Regras de migração**.

   A lista de regras de movimento é exibida.

2. Marque a caixa de seleção ao lado da regra que deseja copiar.
3. Clique em **Copiar**.
4. Na janela que se abre, modifique as seguintes informações na guia **Geral** ou não faça nenhuma modificação se você só quiser copiar a regra sem modificar as suas configurações:

   - Nome da regra

     Digite um nome para a nova regra.

     Se estiver copiando uma regra, a nova regra adquirirá o mesmo nome da regra de origem, mas um índice no formato () será adicionado ao nome, por exemplo: (1).

   - Grupo de administração

     Selecione o grupo de administração para o qual os dispositivos devem ser movidos automaticamente.

   - Regra ativa

     Se esta opção estiver ativada, a regra será ativada e começará a funcionar após ser salva.

     Se esta opção estiver desativada, a regra será criada, mas não ativada. Ela não funcionará até que você ative esta opção.

   - Somente migrar os dispositivos que não pertencem a um grupo de administração

     Se esta opção estiver ativada, somente os dispositivos não atribuídos serão movidos para o grupo selecionado.

     Se esta opção estiver desativada, os dispositivos que já pertencem a outros grupos de administração, bem como os dispositivos não atribuídos, serão movidos para o grupo selecionado.

- Aplicar regra

  Você pode selecionar uma das seguintes opções:

  - **Executar uma vez para cada dispositivo**

    A regra é aplicada uma vez para cada dispositivo que atenda aos critérios.

  - **Executar uma vez para cada dispositivo e depois em cada reinstalação do Agente de Rede**

    A regra é aplicada uma vez para cada dispositivo que atende aos critérios e apenas quando o Agente de Rede é reinstalado nesses dispositivos.

  - **Aplicar regra continuamente**

    A regra é aplicada de acordo com o agendamento que o Servidor de Administração configura automaticamente (normalmente a cada várias horas).

5. Na guia **Condições da regra**, especifique pelo menos um critério para os dispositivos que deseja serem movidos automaticamente.

6. Clique em **Salvar**.

A nova regra de movimentação é criada. Ela é exibida na lista de regras de movimento.

Adicionar dispositivos manualmente a um grupo de administração

É possível mover dispositivos para grupos de administração automaticamente, criando regras de movimentação de dispositivos, ou manualmente, movendo dispositivos de um grupo de administração para outro, ou adicionando dispositivos a um grupo de administração selecionado. Esta seção descreve como adicionar dispositivos a um grupo de administração manualmente.

Para adicionar manualmente um ou mais dispositivos a um grupo de administração selecionado:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.

2. Clique no link **Caminho atual:** `<caminho atual>` acima da lista.

3. Na janela exibida, selecione o grupo de administração ao qual deseja adicionar os dispositivos.

4. Clique no botão **Adicionar dispositivos**.

   O assistente para Mover dispositivos é iniciado.

5. Faça uma lista dos dispositivos que deseja adicionar ao grupo de administração.

   Só é possível adicionar dispositivos para os quais informações já tenham sido adicionadas ao banco de dados do Servidor de Administração ao conectar o dispositivo ou após a descoberta de dispositivos.

   Selecione como deseja adicionar dispositivos à lista:

   - Clique no botão **Adicionar dispositivos** e especifique os dispositivos de uma das seguintes maneiras:

     - Selecione dispositivos na lista de dispositivos detectados pelo Servidor de Administração.

- Especifique o endereço IP de um dispositivo ou um conjunto de IPs.
- Especifique o nome NetBIOS ou o nome DNS de um dispositivo.

  O campo do nome do dispositivo não deve caracteres de espaço, retorno nem os seguintes caracteres proibidos: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Clique no botão **Importar dispositivos do arquivo** para importar uma lista de dispositivos a partir de um arquivo .txt. Cada endereço ou nome de dispositivo deve ser especificado em uma linha separada.

  O arquivo não deve conter caracteres de espaços, retrocessos nem os seguintes caracteres proibidos: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

6. Veja a lista de dispositivos a serem adicionados ao grupo de administração. É possível editar a lista adicionando ou removendo dispositivos.
7. Depois de garantir que a lista esteja correta, clique no botão **Avançar**.

O assistente processa a lista de dispositivos e exibe o resultado. Os dispositivos processados com sucesso são adicionados ao grupo de administração e exibidos na lista de dispositivos sob nomes gerados pelo Servidor de Administração.

Migrando dispositivos ou clusters manualmente para um grupo de administração

Você pode mover dispositivos de um grupo de administração para outro ou do grupo de dispositivos não atribuídos para um grupo de administração.

É possível também mover clusters ou matrizes de servidor de um grupo de administração para outro. Ao mover um cluster ou matriz de servidores para outro grupo, todos os seus nós são movidos com ele, porque um cluster e qualquer um de seus nós sempre pertencem ao mesmo grupo de administração. Quando um único nó de cluster é selecionado na guia **Dispositivos**, o botão **Migrar para grupo** fica indisponível.

Para migrar um ou diversos dispositivos ou clusters em um grupo de administração selecionado:

1. Abra o grupo de administração do qual você deseja migrar os dispositivos. Para fazer isso, execute um dos seguintes procedimentos:
   - Para abrir um grupo de administração, no menu principal, vá para **Ativos (dispositivos)** → **Grupos <nome de grupo>** → **Dispositivos gerenciados**.
   - Para abrir o grupo **Dispositivos não atribuídos**, no menu principal, vá para **Descoberta e implementação** → **Dispositivos não atribuídos**.
2. Caso o grupo de administração contenha clusters ou matrizes de servidores, a seção **Dispositivos gerenciados** será dividida em duas guias – a guia **Dispositivos** e a guia **Grupamentos e matrizes de servidores**. Abra a guia do objeto que deseja mover.
3. Marque a caixa de seleção ao lado dos dispositivos ou clusters que deseja migrar para um grupo diferente.

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

5. Na hierarquia de grupos de administração, marque a caixa de seleção ao lado do grupo de administração para o qual deseja migrar os dispositivos ou clusters selecionados.

6. Clique no botão **Migrar**.

Os dispositivos ou clusters selecionados são movidos para o grupo de administração selecionado.

Configuração de regras de retenção para dispositivos não atribuídos

Após a conclusão da sondagem de rede do Windows, os dispositivos encontrados são colocados em subgrupos do grupo de administração de Dispositivos não atribuídos. Este grupo de administração pode ser encontrado em **Descoberta e implementação → Descoberta → Domínios do Windows**. A pasta **Domínios do Windows** é o grupo principal. Ele contém grupos denominados segundo os domínios e grupos de trabalho correspondentes encontrados durante a sondagem. O grupo principal também pode conter o grupo de administração de dispositivos móveis. Você pode configurar as regras de retenção dos dispositivos não atribuídos do grupo principal e de cada um dos grupos secundários. As regras de retenção não dependem das configurações de descoberta de dispositivos e funcionam mesmo se a descoberta de dispositivos estiver desativada.

As regras de retenção de dispositivo não afetam os dispositivos que têm uma ou mais unidades criptografadas com criptografia completa do disco. Esses dispositivos não são excluídos automaticamente. Somente é possível excluí-los manualmente. Caso necessite excluir um dispositivo com uma unidade criptografada, primeiro descriptografe a unidade e, em seguida, exclua o dispositivo.

Para configurar as regras de retenção para dispositivos não atribuídos:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Domínios do Windows**.

2. Execute uma das seguintes ações:

   - Para definir configurações do grupo principal, clique no botão **Propriedades**.

     A janela Propriedades do domínio do Windows é exibida.

   - Para definir configurações de um grupo secundário, clique no nome do grupo.

     A janela Propriedades do grupo secundário é aberta.

3. Defina as seguintes configurações:

   - **Remover o dispositivo do grupo se estiver inativo por mais de (dias)**

     Se esta opção estiver selecionada, você poderá especificar o intervalo de tempo após o qual o dispositivo será automaticamente removido do grupo. Por padrão, esta opção também é distribuída aos grupos secundários. O intervalo de tempo predefinido é de 7 dias.

     Por padrão, esta opção está ativada.

   - **Herdar do grupo principal**

Se esta opção estiver ativada, o período de retenção para os dispositivos no grupo atual é herdado do grupo principal e não pode ser alterado.

Esta opção está disponível somente para grupos secundários.

Por padrão, esta opção está ativada.

- **Forçar herança em grupos secundários**

  Os valores de configuração serão distribuídos aos grupos secundários, mas essas configurações são bloqueadas nas propriedades dos grupos secundários.

  Por padrão, esta opção está desativada.

4. Clique no botão **Aceitar**.

As suas alterações serão salvas e aplicadas.

Configuração da proteção da rede

Esta seção contém informações sobre a configuração manual de políticas e tarefas, funções de usuário, criação de uma estrutura de grupo de administração e hierarquia de tarefas.

Cenário: Configurar a proteção da rede

O Assistente de início rápido cria políticas e tarefas com as configurações padrão. Essas configurações podem ficar abaixo do ideal ou até mesmo não serem permitidas pela organização. Portanto, recomendamos que você ajuste essas políticas e tarefas e crie outras, se necessárias para a sua rede.

Pré-requisitos

Antes de começar, verifique se você concluiu o cenário de configuração inicial do Kaspersky Security Center Cloud Console, incluindo o Assistente de início rápido.

Quando o Assistente de início rápido estiver em execução, as seguintes políticas e tarefas são criadas no grupo de administração **Dispositivos gerenciados**:

- Política do Kaspersky Endpoint Security
- Tarefa de grupo para atualizar o Kaspersky Endpoint Security
- Política de Agente de Rede
- As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias (tarefa do Agente de Rede)

Fases

A configuração da proteção de rede continua em fases:

1. **Configuração e propagação de políticas e perfis da política de aplicativos Kaspersky**

   Para configurar e propagar as configurações dos aplicativos da Kaspersky instalados nos dispositivos gerenciados, você pode usar duas abordagens de gerenciamento de segurança diferentes: centrado no dispositivo ou centrado no usuário. Você também pode combinar essas duas abordagens.

2. **Configuração de tarefas de gerenciamento remoto de aplicativos Kaspersky**

   Verifique as tarefas criadas com o Assistente de início rápido e faça o ajuste fino delas, se necessário.

   Instruções de como proceder:

   - Configurar a tarefa de grupo para atualizar o Kaspersky Endpoint Security
   - Criar uma tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*

   Se necessário, crie tarefas adicionais para gerenciar os aplicativos da Kaspersky instalados nos dispositivos cliente.

3. **Avaliação e limitação da carga de eventos no banco de dados**

As informações sobre eventos durante a operação de aplicativos gerenciados são transferidas a partir de um dispositivo cliente e registradas no banco de dados do Servidor de Administração. Para reduzir a carga do Servidor de Administração, avalie e limite o número máximo de eventos que podem ser armazenados no banco de dados.

Instruções: Configurando o número máximo de eventos.

Resultados

Quando você concluir esse cenário, sua rede estará protegida pela configuração de aplicativos, tarefas e eventos da Kaspersky recebidos pelo Servidor de Administração:

- Os aplicativos Kaspersky são configurados de acordo com as políticas e perfis de política.
- Os aplicativos são gerenciados através de um conjunto de tarefas.
- O número máximo de eventos que podem ser armazenados no banco de dados está definido.

Quando a configuração da proteção de rede for concluída, você poderá prosseguir para configurar atualizações regulares para bancos de dados e aplicativos Kaspersky.

Sobre as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário

Você pode gerenciar configurações de segurança do ponto de vista de recursos de dispositivo e do ponto de vista de funções de usuário. A primeira abordagem é chamada de *gerenciamento de segurança centrado no dispositivo*, e a segunda, *gerenciamento de segurança centrado no usuário*. Para aplicar configurações diferentes a dispositivos diferentes, é possível usar um dos tipos de gerenciamento ou ambos em conjunto.

O gerenciamento de segurança centralizado no dispositivo permite aplicar diferentes configurações de aplicativos de segurança aos dispositivos gerenciados, dependendo dos recursos específicos do dispositivo. Por exemplo, você pode aplicar configurações diferentes aos dispositivos alocados em diferentes grupos de administração. Você também pode diferenciar os dispositivos usando esses dispositivos no Active Directory ou suas especificações de hardware.

O gerenciamento de segurança centralizado no usuário permite aplicar diferentes configurações do aplicativo de segurança à diferentes funções do usuário. Você pode criar várias funções de usuário, atribuir uma função de usuário apropriada á cada usuário e definir configurações de aplicativos diferentes para os dispositivos pertencentes a usuários com funções diferentes. Por exemplo, convém aplicar configurações do aplicativo diferentes nos dispositivos de contadores e especialistas em recursos humanos (RH). Como resultado, quando o gerenciamento de segurança centrado no usuário é implementado, cada departamento, o departamento de contas e o departamento de RH, têm a sua própria configuração para os aplicativos Kaspersky. Uma configuração define qual configuração do aplicativo pode ser modificada pelos usuários e que são impostas e bloqueadas pelo administrador.

gerenciamento de segurança centrado no usuário, você pode aplicar configurações de aplicativo específicas a usuários individuais. Isso pode ser necessário quando um funcionário tem uma função única na empresa ou quando o usuário quer monitorar os problemas de segurança relacionados aos dispositivos de uma pessoa específica. Dependendo da função desse funcionário na empresa, você pode expandir ou limitar os direitos dessa pessoa para alterar as configurações do aplicativo. Por exemplo, é possível expandir os direitos de um administrador do sistema que gerencia dispositivos cliente em um escritório local.

Você também pode combinar as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário. Por exemplo, você pode configurar uma política de aplicativo específica para cada grupo de administração e, adicionalmente, criar perfis de política para uma ou várias funções dos usuários da sua empresa. Nesse caso, as políticas e os perfis de política são aplicados na seguinte ordem:

1. As políticas criadas para o gerenciamento de segurança centrado no dispositivo são aplicadas.
2. Elas são modificadas pelos perfis de política segundo as prioridades de perfil de política.
3. As políticas são modificadas pelos perfis de política associados às funções de usuário.

Configuração e propagação de políticas: abordagem centrada no dispositivo

Esta seção apresenta o cenário de uma abordagem centrada no dispositivo da configuração centralizada de aplicativos da Kaspersky instalados nos dispositivos gerenciados. Quando você concluir este cenário, os aplicativos serão configurados em todos os dispositivos gerenciados em conformidade com as políticas de aplicativo e perfis da política definidos por você.

Você pode também considerar o gerenciamento de segurança centrado no usuário como uma alternativa ou opção adicional à abordagem centrada no dispositivo.

Processar

O cenário de gerenciamento centrado no dispositivo dos aplicativos Kaspersky consiste nas seguintes etapas:

1. **Configurar os políticas de aplicativo**

   Defina as configurações para aplicativos da Kaspersky instalados nos dispositivos gerenciados por meio da criação de uma política para cada aplicativo. Esse conjunto de políticas será propagado para os dispositivos cliente.

   Quando você configura a proteção da sua rede no Assistente de início rápido, o Kaspersky Security Center Cloud Console cria a política padrão do Kaspersky Endpoint Security for Windows. Se tiver concluído o processo de configuração usando este assistente, você não precisará criar uma nova política para este aplicativo. Prossiga para a configuração manual da política do Kaspersky Endpoint Security.

   Se tiver uma estrutura hierárquica de vários grupos de administração, os grupos de administração secundários herdarão as políticas do Servidor de Administração principal por padrão. Você pode forçar a herança pelos grupos secundários para proibir qualquer modificação das configurações definidas na política de fluxo acima. Se você quiser que somente uma parte das configurações seja herdada por imposição, poderá bloqueá-las na política de fluxo acima. O restante das configurações desbloqueadas ficará disponível para modificação nas políticas de fluxo abaixo. A hierarquia de políticas criada permite que você gerencie dispositivos nos grupos de administração com mais eficiência.

   Instruções de como proceder: Criação de uma política

2. **Criar os perfis da política (opcional)**

   Se você quiser que os dispositivos em um único grupo de administração seja executado sob diferentes configurações de política, crie perfis de políticas para esses dispositivos. Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos alvo em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo gerenciado.

Usando condições de ativação do perfil, você pode aplicar diferentes perfis de políticas, por exemplo, nos dispositivos localizados em uma unidade ou grupo de segurança específico do Active Directory, ter configuração de hardware específica ou marcada com tags específicas. Use tags para filtrar dispositivos que atendem a critérios específicos. Por exemplo, você pode criar um identificador denominado *Windows*, marcar todos os dispositivos executando o sistema operacional Windows com esse identificador e especificar esse identificador como uma condição de ativação para um perfil da política. Como resultado, os aplicativos Kaspersky instalados em todos os dispositivos executando o Windows serão gerenciados por seu próprio perfil da política.

Instruções de como proceder:

- Criar um perfil da política
- Criar uma regra de ativação do perfil da política

3. **Propagar políticas e perfil da política para os dispositivos gerenciados**

   O Kaspersky Security Center Cloud Console sincroniza automaticamente várias vezes por hora o Servidor de Administração com os dispositivos gerenciados. Durante a sincronização, as políticas novas ou alteradas e os perfis da política são propagados para os dispositivos gerenciados. Você pode ignorar a auto sincronização e executar a sincronização manualmente usando o comando Forçar a sincronização. Quando a sincronização estiver concluída, as políticas e os perfis da política serão entregues e aplicados aos aplicativos Kaspersky instalados.

   Você pode verificar se as políticas e os perfis da política foram entregues a um dispositivo. O Kaspersky Security Center Cloud Console especifica a data e hora de entrega nas propriedades do dispositivo.

   Instruções de como proceder: Sincronização forçada

Resultados

Quando o cenário centrado no dispositivo for concluído, os aplicativos Kaspersky serão configurados segundo as configurações especificadas e propagadas por meio da hierarquia de políticas.

As políticas e perfis da política de aplicativo configuradas serão aplicadas automaticamente aos novos dispositivos adicionados aos grupos de administração.

Configuração e propagação de políticas: abordagem centrada no usuário

Esta seção descreve o cenário da abordagem centrada no usuário para configuração centralizada de aplicativos da Kaspersky instalados nos dispositivos gerenciados. Quando você concluir este cenário, os aplicativos serão configurados em todos os dispositivos gerenciados em conformidade com as políticas de aplicativo e perfis da política definidos por você.

Você pode também considerar o gerenciamento de segurança centrado no dispositivo como uma alternativa ou opção adicional à abordagem centrada no usuário. Saiba mais sobre duas abordagens de gerenciamento.

Processar

O cenário de gerenciamento centrado no usuário dos aplicativos da Kaspersky consiste nas seguintes etapas:

1. **Configurar os políticas de aplicativo**

   Defina as configurações para aplicativos Kaspersky instalados nos dispositivos gerenciados por meio da criação de uma política para cada aplicativo. Esse conjunto de políticas será propagado para os dispositivos cliente.

Quando você configura a proteção da sua rede no Assistente de início rápido, o Kaspersky Security Center Cloud Console cria a política padrão do Kaspersky Endpoint Security. Se tiver concluído o processo de configuração usando este assistente, você não precisará criar uma nova política para este aplicativo. Prossiga para a configuração manual da política do Kaspersky Endpoint Security.

Se tiver uma estrutura hierárquica de vários grupos de administração, os grupos de administração secundários herdarão as políticas do Servidor de Administração principal por padrão. Você pode forçar a herança pelos grupos secundários para proibir qualquer modificação das configurações definidas na política de fluxo acima. Se você quiser que somente uma parte das configurações seja herdada por imposição, poderá bloqueá-las na política de fluxo acima. O restante das configurações desbloqueadas ficará disponível para modificação nas políticas de fluxo abaixo. A hierarquia de políticas criada permite que você gerencie dispositivos nos grupos de administração com mais eficiência.

Instruções de como proceder: Criação de uma política

2. **Especificar proprietários dos dispositivos**

   Atribua os dispositivos gerenciados aos usuários correspondentes.

   Instruções de como proceder: Atribuição de um usuário como proprietário do dispositivo

3. **Definir funções do usuário típicas para a sua empresa**

   Pense sobre diferentes tipos de trabalhos que os funcionários da sua empresa normalmente executam. Você deve dividir todos de acordo com as funções. Por exemplo, você pode dividi-los por departamentos, profissões ou cargos. Depois disso, você precisará criar uma função do usuário para cada grupo. Tenha em mente que cada função do usuário terá seu próprio perfil da política contendo configurações do aplicativo específicas para essa função.

4. **Criar funções de usuário**

   Crie e configure uma função do usuário para cada grupo de funcionários que você definiu na etapa anterior ou use as funções do usuário predefinidas. As funções do usuário conterão o conjunto de direitos de acesso aos recursos do aplicativo.

   Instruções de como proceder: Criação de uma função de usuário

5. **Especificar o escopo de cada função de usuário**

   Para cada uma das funções de usuário criadas, defina usuários e/ou grupos de segurança e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

   Instruções de como proceder: Edição do escopo de uma função de usuário

6. **Criar os perfis da política**

   Crie um perfil da política para cada função de usuário em sua empresa. Os perfis da política definem quais configurações serão aplicadas aos aplicativos instalados em dispositivos de usuários dependendo da função de cada usuário.

   Instruções de como proceder: Criação de um perfil da política

7. **Associar perfis da política com as funções do usuário**

   Associe os perfis de política criados com as funções do usuário. Depois disso: o perfil da política fica ativo para um usuário com a função especificada. As configurações definidas no perfil da política serão aplicadas aos aplicativos da Kaspersky instalados nos dispositivos do usuário.

   Instruções de como proceder: Associar perfis da política a funções

8. **Propagar políticas e perfil da política para os dispositivos gerenciados**

O Kaspersky Security Center Cloud Console sincroniza automaticamente várias vezes por hora o Servidor de Administração com os dispositivos gerenciados. Durante a sincronização, as políticas novas ou alteradas e os perfis da política são propagados para os dispositivos gerenciados. Você pode ignorar a auto sincronização e executar a sincronização manualmente usando o comando Forçar a sincronização. Quando a sincronização estiver concluída, as políticas e os perfis da política serão entregues e aplicados aos aplicativos Kaspersky instalados.

Você pode verificar se as políticas e os perfis da política foram entregues a um dispositivo. O Kaspersky Security Center Cloud Console especifica a data e hora de entrega nas propriedades do dispositivo.

Instruções de como proceder: Sincronização forçada

Resultados

Quando o cenário centrado no usuário for concluído, os aplicativos da Kaspersky serão configurados segundo as configurações especificadas e propagadas por meio da hierarquia de políticas e perfis de política.

Para um novo usuário, você terá de criar uma nova conta, atribuir o usuário com uma das funções de usuário criadas e atribuir os dispositivos ao usuário. As políticas e perfis da política de aplicativo configuradas serão automaticamente aplicadas aos novos dispositivos adicionados aos dispositivos de esse usuário.

Configuração manual da política do Kaspersky Endpoint Security

Esta seção fornece recomendações sobre como configurar a política do Kaspersky Endpoint Security. É possível executar a configuração na janela de propriedades da política. Ao editar uma configuração, clique no ícone de cadeado à direita do grupo relevante de configurações para aplicar os valores especificados a uma estação de trabalho.

Configurar a Kaspersky Security Network

A Kaspersky Security Network (KSN) é a infraestrutura de serviços em nuvem que possui informações sobre a reputação de arquivos, recursos da Web e software. A Kaspersky Security Network permite que o Kaspersky Endpoint Security for Windows responda mais rapidamente a diferentes tipos de ameaças, melhore o desempenho dos componentes de proteção e reduza a probabilidade de falsos positivos. Para obter mais informações sobre a Kaspersky Security Network, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

É possível configurar o trabalho do Kaspersky Security Network na janela de propriedades da política do Kaspersky Endpoint Security for Windows, na seção **Configurações do aplicativo** → **Proteção avançada contra ameaças**.

Para especificar as configurações recomendadas de KSN:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique na política do Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política selecionada é aberta.
3. Nas propriedades de política, acesse **Configurações do aplicativo** → **Proteção Avançada Contra Ameaças** → **Kaspersky Security Network**.
4. Verifique e confirme se a opção **Usar o Servidor de Administração como servidor proxy da KSN** está ativada. Use esse recurso para redistribuir e otimizar o tráfego na rede.

Se você usar Detection and Response gerenciadas, ative a opção **Proxy KSN** para o ponto de distribuição e ativar o modo KSN estendido.

5. [opcional] Ativar o uso de servidores KSN se o serviço de proxy da KSN não estiver disponível. Para fazer isso, ative a opção **Usar servidores da Kaspersky Security Network se o servidor proxy da KSN estiver indisponível**.

   Os servidores KSN podem estar localizados no lado da Kaspersky (quando a KSN é usada) ou no lado de terceiros (quando a KPSN é usada).

6. Clique em **OK**.

As configurações de KSN recomendadas são especificadas.

Verificação da lista das redes protegidas por Firewall

Verifique se o Firewall do Kaspersky Endpoint Security for Windows protege todas as redes. Por padrão, o Firewall protege as redes com os seguintes tipos de conexão:

- **Rede pública**. Aplicativos antivírus, firewalls ou filtros não protegem os dispositivos dessa rede.
- **Rede local**. O acesso a arquivos e impressoras é restrito para dispositivos nesta rede.
- **Rede confiável**. Os dispositivos dessa rede são protegidos contra ataques e acesso não autorizado a arquivos e dados.

Se você configurou uma rede personalizada, certifique-se de ela esteja protegida por Firewall. Para isso, verifique a lista de redes nas propriedades da política do Kaspersky Endpoint Security for Windows. A lista pode não conter todas as redes.

Para obter mais informações sobre o Firewall, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

Para verificar a lista de redes:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique na política do Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política selecionada é aberta.

3. Nas propriedades de política, acesse **Configurações do aplicativo** → **Proteção Essencial Contra Ameaças** → **Firewall**.
4. Em **Redes disponíveis**, clique no link **Configurações de rede**.

   A janela de **Conexões de rede** é aberta. Esta janela exibe a lista de redes.

5. Caso a lista tenha uma rede ausente, basta adicioná-la.

Excluir detalhes de software da memória do Servidor de Administração

Recomendamos que o Servidor de Administração não salve as informações sobre módulos de software que sejam iniciados nos dispositivos de rede. Como resultado, a memória do Servidor de Administração não ficará sobrecarregada.

É possível desabilitar o salvamento dessas informações nas propriedades de política do Kaspersky Endpoint Security for Windows.

Para desativar a gravação de informações sobre os módulos de software instalados:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique na política do Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política selecionada é aberta.
3. Nas propriedades de política, acesse **Configurações do aplicativo** → **Configurações Gerais** → **Relatórios e Armazenamentos**.
4. Em **Transferência de dados para o Servidor de Administração**, desmarque a caixa de seleção **Sobre os aplicativos iniciados** se ainda estiver marcada na política de nível superior.

   Quando esta caixa de seleção for marcada, o banco de dados do Servidor de Administração salvará as informações sobre todas as versões de todos os módulos do software nos dispositivos em rede. Estas informações podem necessitar de uma quantidade significativa do espaço disponível em disco para o banco de dados do Kaspersky Security Center Cloud Console (dúzias de gigabytes).

As informações sobre módulos de software instalados não são mais salvas no banco de dados do Servidor de Administração.

Salvar eventos de política importantes no banco de dados do Servidor de Administração

Para evitar a sobrecarga do banco de dados do Servidor de Administração, recomendamos que você salve apenas os eventos importantes no banco de dados.

Para configurar o registro de eventos importantes no banco de dados do Servidor de Administração:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique na política do Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política selecionada é aberta.
3. Nas propriedades da política, abra a guia **Configuração de eventos**.
4. Na seção **Crítico**, clique em **Adicionar evento** e marque as caixas de seleção ao lado dos seguintes eventos apenas:

   - *Contrato de licença de usuário final violado*
   - *A execução automática do aplicativo está desativada*
   - *Erro de ativação*
   - *Ameaça ativa detectada. A Desinfecção Avançada deve ser iniciada*

- *Desinfecção impossível*
- *Link perigoso aberto anteriormente detectado*
- *Processo concluído*
- *Atividade de rede bloqueada*
- *Ataque de rede detectado*
- *Proibida a inicialização do aplicativo*
- *Acesso negado (bases locais)*
- *Acesso negado (KSN)*
- *Erro de atualização local*
- *Não foi possível iniciar duas tarefas ao mesmo tempo*
- *Erro na interação com o Kaspersky Security Center*
- *Nem todos os componentes foram atualizados*
- *Erro ao aplicar as regras de criptografia/descriptografia*
- *Erro ao ativar o modo portátil*
- *Erro ao desativar o modo portátil*
- *Não foi possível carregar o módulo de criptografia*
- *A política não pode ser aplicada*
- *Erro ao alterar os componentes do aplicativo*

5. Clique em **OK**.
6. Na seção **Falha funcional**, clique em **Adicionar evento** e marque apenas as caixas de seleção ao lado de *Configurações de tarefa inválidas do evento. Configurações não aplicadas*.
7. Clique em **OK**.
8. Na seção **Advertência**, clique em **Adicionar evento** e marque as caixas de seleção ao lado dos seguintes eventos apenas:
   - *Autodefesa desativada*
   - *Componentes de proteção estão desativados*
   - *Chave de reserva incorreta*
   - *Software legítimo que pode ser usado por intrusos para danificar o computador ou dados pessoais foi detectado (bases locais)*

- *Software legítimo que pode ser usado por intrusos para danificar o computador ou dados pessoais foi detectado (KSN)*
- *Objeto excluído*
- *Objeto desinfectado*
- *O usuário optou por não usar a política de criptografia*
- *O arquivo foi restaurado a partir da quarentena no servidor da Kaspersky Anti Targeted Attack Platform pelo administrador*
- *O arquivo foi colocado em quarentena no servidor da Kaspersky Anti Targeted Attack Platform pelo administrador*
- *Mensagem para o administrador sobre a proibição de inicialização do aplicativo*
- *Mensagem para o administrador sobre a proibição de acesso ao dispositivo*
- *Mensagem para o administrador sobre a proibição de acesso à página da Web*

9. Clique em **OK**.
10. Na seção **Informações**, clique em **Adicionar evento** e marque as caixas de seleção ao lado dos seguintes eventos apenas:
    - *Foi criada uma cópia de backup do objeto*
    - *Proibida a inicialização do aplicativo em modo de teste*
11. Clique em **OK**.

O registro de eventos importantes no banco de dados do Servidor de Administração é configurado.

Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security

A opção de agendamento ideal e recomendada para o Kaspersky Endpoint Security é **Quando novas atualizações são baixadas no repositório** quando a caixa de seleção **Usar atraso aleatório automaticamente para início da tarefa** estiver marcada.

Tarefas

Esta seção descreve as tarefas utilizadas pelo Kaspersky Security Center Cloud Console.

Sobre as tarefas

O Kaspersky Security Center Cloud Console gerencia os aplicativos de segurança Kaspersky instalados nos dispositivos cliente criando e executando tarefas. As *tarefas* são necessárias para a instalação, inicialização e interrupção de aplicativos, verificação de arquivos, atualização de bancos de dados e módulos de software e para a realização de outras ações em aplicativos. As tarefas podem ser realizadas no Servidor de Administração e em dispositivos.

Os seguintes tipos de tarefas são executados nos dispositivos:

- *Tarefas locais* – Tarefas que são executadas em um dispositivo específico

  As tarefas locais podem ser modificadas pelo administrador, usando as ferramentas de administração, ou pelo usuário de um dispositivo remoto (por exemplo, através da interface do aplicativo de segurança). Se uma tarefa local tiver sido modificada simultaneamente pelo administrador e pelo usuário de um dispositivo gerenciado, as modificações feitas pelo administrador entrarão em vigor porque elas têm uma maior prioridade.

- *Tarefas de grupo* – Tarefas que são executadas em todos os dispositivos de um grupo específico

  Salvo de especificado de outra maneira nas propriedades de tarefa, uma tarefa de grupo também afeta todos os subgrupos do grupo selecionado.

- *Tarefas globais* – Tarefas que são realizadas em um conjunto de dispositivos, independentemente se os mesmos estão incluídos em qualquer grupo

Para cada aplicativo, você pode criar diversas tarefas de grupo, tarefas globais ou tarefas locais.

Você pode efetuar alterações nas configurações de tarefas, exibir o andamento das tarefas, copiar, exportar, importar e excluir tarefas.

Uma tarefa é iniciada em um dispositivo cliente somente se um aplicativo para o qual a tarefa foi criada estiver sendo executado.

Os resultados da execução das tarefas são salvos no log de eventos do SO em cada dispositivo e no banco de dados do Servidor de Administração.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Sobre o escopo de tarefa

O *escopo de uma tarefa* é o conjunto de dispositivos nos quais a tarefa é executada. Os tipos de escopo são os seguintes:

- Para uma *tarefa local*, o escopo é o próprio dispositivo.
- Para uma tarefa do *Servidor de Administração*, o escopo é o Servidor de Administração.
- Para uma *tarefa de grupo*, o escopo é a lista de dispositivos incluídos no grupo.

Ao criar uma *tarefa global*, você pode usar os seguintes métodos para especificar o escopo:

- Especificar determinados dispositivos manualmente.

Você pode usar um endereço IP (ou uma faixa IP), nome NetBIOS ou nome DNS como o endereço do dispositivo.

- Importar uma lista de dispositivos de um arquivo TXT com os endereços dos dispositivos a serem adicionados (cada endereço deve ser colocado em uma linha individual).

  Se você importar uma lista de dispositivos a partir de um arquivo ou cria uma lista manualmente, e se os dispositivos cliente estão identificados pelos seus nomes, a lista deve conter somente os dispositivos cuja informação já foi adicionada ao banco de dados do Servidor de Administração. Além disso, as informações devem ter sido inseridas quando os dispositivos foram conectados ou durante a descoberta de dispositivos.

- Especificar uma seleção de dispositivos.

  Ao longo do tempo, o escopo de uma tarefa se modifica quando o conjunto de dispositivos incluídos na seleção são modificados. Uma seleção de dispositivos pode ser feita com base nos atributos do dispositivo, incluindo o software instalado em um dispositivo, e com base em tags atribuídas aos dispositivos. A seleção de dispositivos é o modo mais flexível para especificar o escopo de uma tarefa.

  As tarefas para seleções de dispositivos sempre são executadas de acordo com um agendamento pelo Servidor de Administração. Estas tarefas não podem ser executadas em dispositivos que não tenham uma conexão com o Servidor de Administração. As tarefas cujo escopo é especificado por outros métodos são executadas diretamente nos dispositivos e, por isso, não dependem da conexão do dispositivo com o Servidor de Administração.

As tarefas para Seleções de dispositivos não são executadas na hora local de um dispositivo; em vez disso, elas serão executadas na hora local do Servidor de Administração. As tarefas cujo escopo é especificado por outros métodos são executadas na hora local de um dispositivo.

Criar uma tarefa

É possível criar uma tarefa na lista de tarefas. Como alternativa, você pode selecionar dispositivos na lista de **Dispositivos gerenciados** e criar uma nova tarefa atribuída aos dispositivos selecionados.

Para criar uma tarefa na lista de tarefas:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as instruções.
3. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.
4. Clique no botão **Concluir**.

A tarefa é criada e exibida na lista de tarefas.

Para criar uma nova tarefa atribuída aos dispositivos selecionados:

No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.

A lista de dispositivos gerenciados é exibida.

1. Na lista de dispositivos gerenciados, marque as caixas de seleção ao lado dos dispositivos para executar a tarefa para eles. Você pode usar as funções de pesquisa e filtro para encontrar os dispositivos que está

procurando.

2. Clique no botão **Executar tarefa** e selecione **Criar nova tarefa**.

   O Assistente para novas tarefas inicia.

   Na primeira etapa do assistente, você pode remover os dispositivos selecionados para incluir no escopo da tarefa. Siga as instruções do assistente.

3. Clique no botão **Concluir**.

A tarefa é criada para os dispositivos selecionados.

Visualizando a lista de tarefas

Você pode ver a lista de tarefas criadas no Kaspersky Security Center Cloud Console.

Para visualizar a lista de tarefas,

No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.

A lista de tarefas é exibida. As tarefas são agrupadas pelos nomes dos aplicativos aos quais estão relacionados. Por exemplo, a tarefa Desinstalar aplicativo remotamente está relacionada ao Servidor de Administração e a tarefa Encontrar as vulnerabilidades e as atualizações necessárias ao Agente de Rede.

Para visualizar as propriedades de uma tarefa,

Clique no nome da tarefa.

A janela de propriedades da tarefa é exibida com várias guias nomeadas. Por exemplo, **Tipo de tarefa** é exibido na guia **Geral** e o agendamento de tarefas - na guia **Agendamento**.

Como iniciar uma tarefa manualmente

O aplicativo inicia as tarefas de acordo com as configurações de agendamento especificadas nas propriedades de cada tarefa. Você pode iniciar uma tarefa manualmente a qualquer momento por meio da lista de tarefas. Você também pode selecionar dispositivos na lista **Dispositivos gerenciados** e, em seguida, iniciar uma tarefa existente para eles.

Para iniciar uma tarefa manualmente:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.

2. Na lista de tarefas, selecione a caixa de seleção ao lado da tarefa que deseja iniciar.

3. Clique no botão **Iniciar**.

A tarefa é iniciada. Você pode verificar o status da tarefa na coluna **Status** ou clicando no botão **Resultado**.

Como iniciar uma tarefa para dispositivos selecionados

Você pode selecionar um ou mais dispositivos cliente na lista de dispositivos e iniciar uma tarefa criada anteriormente para eles. Isso permite executar tarefas criadas anteriormente para um conjunto específico de dispositivos.

Isso altera os dispositivos aos quais a tarefa foi atribuída para a lista de dispositivos que você seleciona ao executar a tarefa.

Para iniciar uma tarefa para dispositivos selecionados:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**. A lista de dispositivos gerenciados é exibida.

Na lista de dispositivos gerenciados, use as caixas de seleção para selecionar os dispositivos para executar a tarefa para eles. Você pode usar as funções de pesquisa e filtro para encontrar os dispositivos que está procurando.

1. Clique no botão **Executar tarefa** e selecione **Aplicar tarefa existente**.

   A lista de tarefas existentes é exibida.

2. Os dispositivos selecionados são exibidos acima da lista de tarefas. Se necessário, é possível remover um dispositivo dessa lista. Você pode excluir todos os dispositivos, exceto um.

3. Selecione a tarefa desejada na lista. Use a caixa de pesquisa acima da lista para pesquisar a tarefa desejada pelo nome. Apenas uma tarefa pode ser selecionada.

4. Clique em **Salvar e iniciar a tarefa**.

   A tarefa selecionada é iniciada imediatamente para os dispositivos selecionados. As configurações de início agendado na tarefa não são alteradas.

Configurações e propriedades gerais da tarefa

Esta seção contém as configurações que podem ser definidas e especificadas para a maioria das tarefas. A lista de configurações disponíveis depende da tarefa que se está configurando.

Configurações especificadas durante a criação de tarefa

Você pode especificar as seguintes configurações ao criar uma tarefa. Algumas dessas configurações também podem ser modificadas nas propriedades da tarefa criada.

- Dispositivos aos quais a tarefa será atribuída:
  - **Atribuir tarefa a um grupo de administração**

A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

- Especificar endereços de dispositivos manualmente ou importar endereços de uma lista

  A tarefa é atribuída a dispositivos específicos. Você pode especificar dispositivos usando um dos seguintes métodos:

  - Especifique o endereço IP, o nome NetBIOS ou o nome DNS do dispositivo.
  - Especifique o intervalo de IPs.

    Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.
  - Selecione dispositivos detectados pelo Servidor de Administração, incluindo dispositivos não atribuídos.

    Por exemplo, pode ser necessário usar esta opção em uma tarefa de instalação do Agente de Rede em dispositivos não atribuídos.

- Atribuir a tarefa a uma seleção de dispositivos

  A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

  Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

- Configurações de conta:

  - Conta padrão

    A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

    Por padrão, esta opção está selecionada.

  - Especificar conta

    Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

- Configurações para reiniciar o sistema operacional:

  - Não reiniciar

Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

  A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

  Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

  Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

  Por padrão, esta opção está desativada.

Configurações especificadas após a criação da tarefa

Você pode especificar as seguintes configurações após criar uma tarefa.

- Configurações de tarefa de grupo:
  - **Distribuir para subgrupos**

    Essa opção só está disponível nas configurações das tarefas de grupo.

    Quando essa opção está habilitada, o escopo da tarefa inclui:

    - O grupo de administração selecionado ao criar a tarefa.
    - Os grupos de administração subordinados ao grupo de administração selecionado em qualquer nível abaixo na hierarquia do grupo.

    Quando essa opção está desabilitada, o escopo da tarefa inclui apenas o grupo de administração selecionado ao criar a tarefa.

    Por padrão, esta opção está ativada.

  - **Distribuir em Servidores de Administração secundários e virtuais**

    Quando essa opção está habilitada, a tarefa efetiva no Servidor de Administração principal também é aplicada nos Servidores de Administração secundários (incluindo os virtuais). Caso já exista uma tarefa do mesmo tipo no Servidor de Administração secundário, ambas as tarefas serão aplicadas no Servidor de Administração secundário (a existente e a herdada do Servidor de Administração principal).

    Essa opção só está disponível quando a opção **Distribuir para subgrupos** está habilitada.

    Por padrão, esta opção está desativada.

- Configurações de agendamento de tarefas:
  - **Início agendado configuração:**
    - **Manualmente**

      A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

      Por padrão, esta opção está ativada.

    - **A cada N minutos**

      A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

      Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

    - **A cada N horas**

      A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

      Por padrão, a tarefa é executada a cada seis horas, iniciando na data e hora atuais do sistema.

- **A cada N dias**

  A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

  Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

- **A cada N semanas**

  A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

  Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

- **Diariamente (não é compatível com horário de verão)**

  A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

  Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center Cloud Console.

  Por padrão, a tarefa inicia diariamente na hora atual do sistema.

- **Semanalmente**

  A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e na hora especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Todos os meses em dias especificados das semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

- **Quando novas atualizações são baixadas no repositório**

Quando novas atualizações são baixadas nos repositórios de pontos de distribuição, o Kaspersky Security Center Cloud Console executa todas as tarefas que possuem esse agendamento. O Agente de Rede verifica a disponibilidade de atualizações durante a sincronização periódica entre o dispositivo gerenciado e o Servidor de Administração (o heartbeat).

Por exemplo, convém usar esse agendamento para a tarefa de Atualização relacionada a um aplicativo de segurança, como o Kaspersky Endpoint Security.

Se o Agente de Rede em um dispositivo gerenciado não detectar nenhuma nova atualização por 25 horas ou mais, o Kaspersky Security Center Cloud Console executará nesse dispositivo todas as tarefas que têm esse agendamento. Essas tarefas são executadas a cada hora até que novas atualizações sejam detectadas. O Kaspersky Security Center Cloud Console também executa essas tarefas a cada hora se não houver conexão entre o dispositivo gerenciado e o ponto de distribuição que baixa as atualizações no repositório.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Você pode precisar executar tarefas diferentes, dependendo do tipo de aplicativo antivírus que informa um ataque de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

  Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

  Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

  Se esta opção estiver desativada, somente as tarefas agendadas serão executadas nos dispositivos cliente; para **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas somente são executadas naqueles dispositivos cliente que estiverem visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

  Por padrão, esta opção está ativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

Se esta opção for ativada, a tarefa é iniciada nos dispositivos cliente aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos cliente aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

- Usar atraso aleatório para inícios de tarefa em um intervalo de (min.)

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos cliente aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

- Ligar dispositivos usando a função Wake-On-LAN antes de iniciar a tarefa (min.)

  O sistema operacional do dispositivo selecionado inicia na hora especificada, antes do início da tarefa. O período de tempo padrão é de cinco minutos.

  Ative esta opção se você quiser que a tarefa seja executada em todos os dispositivos cliente do escopo da tarefa, inclusive nos dispositivos que são desligados quando a tarefa está prestes a ser iniciada.

  Se você deseja que o dispositivo seja desligado automaticamente após a conclusão da tarefa, ative a opção **Desligar os dispositivos após concluir a tarefa**. Esta opção pode ser encontrada na mesma janela.

  Por padrão, esta opção está desativada.

- Desligar os dispositivos após concluir a tarefa

  Por exemplo, pode ser necessário ativar esta opção para uma tarefa que instala atualizações nos dispositivos cliente todas as sextas-feiras após o horário comercial e, em seguida, desliga esses dispositivos durante o fim de semana.

  Por padrão, esta opção está desativada.

- Parar a tarefa se ela for executada por mais que (min.)

  Após o final do período especificado, a tarefa é interrompida automaticamente, quer tenha sido concluída ou não.

  Ative esta opção se você quiser interromper (ou parar) tarefas que levam muito tempo para serem executadas.

  Por padrão, esta opção está desativada. O tempo predefinido de execução da tarefa é de 120 minutos.

- Notificações:
  - Bloco **Armazenar histórico de tarefas**:
    - **Salvar todos os eventos**
    - **Salvar eventos relacionados ao progresso da tarefa**
    - **Salvar apenas os resultados da execução da tarefa**
    - Armazenar no banco de dados do Servidor de Administração por (dias)

      Os eventos de aplicativo relacionados à execução da tarefa em todos os dispositivos cliente do escopo da tarefa são armazenados no Servidor de Administração durante o número de dias especificado. Quando esse período termina, as informações são excluídas do Servidor de Administração.

      Por padrão, esta opção está ativada.
    - Armazenar no log de eventos do SO no dispositivo

      Os eventos de aplicativo relacionados à execução da tarefa são armazenados localmente no Log de Eventos do Windows de cada dispositivo cliente.

      Por padrão, esta opção está desativada.
  - **Notificar somente erros**
  - **Notificar por e-mail**
- Configurações do escopo da tarefa
- Escopo das exclusões

  Você pode especificar grupos de dispositivos aos quais a tarefa não é aplicada. Os grupos a serem excluídos podem somente ser subgrupos do grupo de administração ao qual a tarefa é aplicada.
- **Histórico de revisões**

Exportação de tarefa

O Kaspersky Security Center Cloud Console permite salvar uma tarefa e suas configurações em um arquivo KLT. Você pode usar este arquivo KLT para importar a tarefa salva tanto para o Kaspersky Security Center Windows quanto para o Kaspersky Security Center Linux.

Para exportar uma tarefa:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Marque a caixa de seleção ao lado da tarefa que deseja exportar.

   Você não pode exportar várias tarefas ao mesmo tempo. Se selecionar mais de uma tarefa, o botão **Exportar** será desabilitado. As tarefas do Servidor de Administração também ficam indisponíveis para exportação.

3. Clique no botão **Exportar**.

4. Na janela **Salvar como** que abrir, especifique o nome e o caminho do arquivo de tarefa. Clique no botão **Salvar**.

   A janela **Salvar como** é exibida apenas se você usar Google Chrome, Microsoft Edge ou Opera. Se usar outro navegador, o arquivo da tarefa será salvo automaticamente na pasta **Downloads**.

Importação de uma tarefa

O Kaspersky Security Center Cloud Console permite importar uma tarefa de um arquivo KLT. O arquivo KLT contém a tarefa exportada e suas configurações.

Para importar uma tarefa:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.

2. Clique no botão **Importar**.

3. Clique no botão **Procurar** para escolher um arquivo de tarefa que você deseja importar.

4. Na janela aberta, especifique o caminho para o arquivo de tarefa KLT e clique no botão **Abrir**. Observe que você pode selecionar apenas um arquivo de tarefa.

   O processamento da tarefa é iniciado.

5. Após o processamento com êxito da tarefa, selecione os dispositivos aos quais deseja atribuir a tarefa. Para fazer isso, selecione uma das seguintes opções:

   - **Atribuir tarefa a um grupo de administração**

     A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

     Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

   - **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**

     Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

     Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

   - **Atribuir a tarefa a uma seleção de dispositivos**

     A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

     Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

6. Especifique o escopo da tarefa.

7. Clique no botão **Concluir** para encerrar a importação da tarefa.

A notificação com os resultados da importação é exibida. Se a tarefa for importada com êxito, será possível clicar no link **Detalhes** para visualizar as propriedades da tarefa.

Após a importação com êxito, a tarefa será exibida na lista de tarefas. As configurações de tarefa e o agendamento também são importados. A tarefa será iniciada de acordo com seu agendamento.

Se a tarefa recém-importada tiver um nome idêntico a uma tarefa existente, o nome da tarefa importada será expandido com o índice **(<próximo número da sequência>)**, por exemplo: **(1)**, **(2)**.

Gerenciamento de dispositivos cliente

Esta seção descreve como gerenciar dispositivos nos grupos de administração.

Configurações de um dispositivo gerenciado

Para exibir as configurações de um dispositivo gerenciado:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo necessário.

   A janela Propriedades do dispositivo selecionado é exibida.

As seguintes guias são exibidas na parte superior da janela de propriedades; elas representam os principais grupos de configurações:

- Geral

Esta guia compreende as seguintes seções:

- A seção **Geral** exibe as informações gerais sobre o dispositivo cliente. As informações são fornecidas com base nos dados recebidos durante a última sincronização do dispositivo cliente com o Servidor de Administração:

  - **Nome**

    Neste campo, você poderá visualizar e modificar o nome de um dispositivo cliente no grupo de administração.

  - **Descrição**

    Nesse campo, você poderá inserir uma descrição adicional de um dispositivo cliente.

  - **Status do dispositivo**

    Status do dispositivo cliente atribuído com base nos critérios definidos pelo administrador para o status de proteção antivírus no dispositivo e na atividade do dispositivo na rede.

  - **Proprietário do dispositivo**

    Nome do proprietário do dispositivo. É possível atribuir ou remover um usuário como proprietário de um dispositivo ao clicar no link **Gerenciar proprietário do dispositivo**.

  - **Nome completo do grupo**

    Grupo de administração que inclui o dispositivo cliente.

  - **Última atualização dos bancos de dados de antivírus**

    Data em que os bancos de dados de antivírus ou os aplicativos foram atualizados pela última vez no dispositivo.

  - **Conectado ao Servidor de Administração**

    Data e hora da última vez que o Agente de Rede instalado no dispositivo cliente foi conectado ao Servidor de Administração.

  - **Última visualização**

    Data e hora de quando o dispositivo esteve por último visível na rede.

  - **Versão do Agente de Rede**

    Versão do Agente de Rede instalado.

- **Criação**

  Data de criação do dispositivo no Kaspersky Security Center Cloud Console.

- **Não desconectar do Servidor de Administração**

  Caso a opção seja ativada, será mantida uma conectividade contínua entre o dispositivo gerenciado e o Servidor de Administração. Convém usar a opção caso os servidores push, que fornecem a conectividade, não estejam sendo usados.

  Caso essa opção esteja desativada e os servidores push não estejam sendo utilizados, o dispositivo gerenciado somente se conectará ao Servidor de Administração para sincronizar dados ou transmitir informações.

  O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

  A opção é desativada por padrão em dispositivos gerenciados. A opção é ativada por padrão no dispositivo onde o Servidor de Administração está instalado e permanece ativada mesmo se você tentar desativá-la.

- A seção **Rede** exibe as seguintes informações sobre as propriedades da rede do dispositivo cliente:

  - **Endereço IP**

    Endereço IP do dispositivo.

  - **Domínio do Windows**

    O domínio do Windows ou o grupo de trabalho, que contém o dispositivo.

  - **Nome DNS**

    Nome do domínio DNS do dispositivo cliente.

  - **Nome do NetBIOS**

    Nome de rede Windows do dispositivo cliente.

  - **Endereço IPv6**

- A seção **Sistema** fornece informações sobre o sistema operacional instalado no dispositivo cliente:

  - **Sistema operacional**
  - **Arquitetura da CPU**
  - **Desenvolvedor do SO**
  - **Pasta do sistema operacional**
  - **Nome do dispositivo**

- Tipo de máquina virtual

  O fabricante da máquina virtual.

- Máquina virtual dinâmica como parte da VDI

  Esta seta exibe se o dispositivo cliente é uma máquina virtual dinâmica como parte da VDI.

- **Compilação do sistema operacional**

- A seção **Proteção** fornece as seguintes informações sobre o status atual da proteção antivírus no dispositivo cliente:

  - Visível

    O status da visibilidade do dispositivo cliente.

  - Status do dispositivo

    Status do dispositivo cliente atribuído com base nos critérios definidos pelo administrador para o status de proteção antivírus no dispositivo e na atividade do dispositivo na rede.

  - Descrição de status

    Status da proteção do dispositivo cliente e conexão com o Servidor de Administração.

  - Status da proteção

    Esse campo exibe o status atual da proteção em tempo real do dispositivo cliente.

    Quando o status é alterado no dispositivo, o novo status é exibido na janela de propriedades do dispositivo só depois que o dispositivo cliente é sincronizado com o Servidor de Administração.

  - Última verificação completa

    Data e hora em que a verificação de malwares foi executada por último no dispositivo cliente.

  - Vírus detectado

    Número total de ameaças detectadas no dispositivo cliente desde a instalação do aplicativo antivírus (primeira verificação) ou desde o último reinício do contador de ameaças.

  - Objetos com desinfecção mal-sucedida

    Número de arquivos não processados no dispositivo cliente.

    Este campo ignora o número de arquivos não processados nos dispositivos móveis.

  - Status de criptografia do disco

O status atual da criptografia do arquivo nas unidades locais do dispositivo. Para obter uma descrição dos status, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

- A seção **Status do dispositivo definido pelo aplicativo** fornece informações sobre o status do dispositivo definido pelo aplicativo gerenciado e instalado no dispositivo. O status do dispositivo pode ser diferente do definido pelo Kaspersky Security Center Cloud Console.

- Aplicativos

  Esta seção lista todos os aplicativos da Kaspersky instalados no dispositivo cliente. É possível clicar no nome do aplicativo para visualizar informações gerais sobre o aplicativo, uma lista de eventos que ocorreram no dispositivo e as configurações do aplicativo.

- Políticas e perfis de política ativos

  Esta seção lista as políticas e perfis de políticas atualmente ativos no dispositivo gerenciado.

- Tarefas

  Na guia **Tarefas**, é possível gerenciar as tarefas do dispositivo cliente: visualizar a lista de tarefas existentes, criar novas, remover, iniciar e interromper tarefas, modificar as suas configurações e visualizar os resultados da execução. A lista de tarefas é fornecida com base nos dados recebidos durante a última sessão de sincronização do cliente com o Servidor de Administração. O Servidor de Administração solicita os detalhes do status de tarefa do dispositivo cliente. Se a conexão não é estabelecida, o status não é exibido.

- Eventos

  A guia **Eventos** exibe os eventos registrados no Servidor de Administração para o dispositivo cliente selecionado.

- Incidentes

  Na guia **Incidentes**, é possível visualizar, editar e criar problemas de segurança para o dispositivo cliente. Os problemas de segurança podem ser criados automaticamente pelos aplicativos da Kaspersky gerenciados e instalados no dispositivo cliente ou manualmente pelo administrador. Por exemplo, caso alguns usuários movam regularmente malwares de suas unidades removíveis para os dispositivos, o administrador poderá criar um problema de segurança. No texto do problema de segurança, o administrador pode fornecer uma breve descrição do caso e as ações recomendadas (como ações disciplinares a serem tomadas contra um usuário) e pode adicionar um link para o usuário ou usuários.

  Um problema de segurança para o qual todas as ações necessárias foram tomadas é chamado de *processado*. A presença de problemas de segurança não processados pode ser escolhida como a condição para uma alteração do status do dispositivo para *Crítico* ou *Advertência*.

  Esta seção contém uma lista de problemas de segurança que foram criados para o dispositivo. Os problemas de segurança são classificados por nível de gravidade e tipo. O tipo de problema de segurança é definido pelo aplicativo da Kaspersky, que cria o problema de segurança. É possível destacar os problemas de segurança processados na lista ao marcar a caixa de seleção na coluna **Processed**.

- Tags

Na guia **Tags**, é possível gerenciar a lista de palavras-chave que são usadas para localizar os dispositivos cliente: visualizar a lista de tags existentes, atribuir tags a partir da lista, configurar regras de identificação automática, adicionar novas tags, renomear as antigas e excluir tags.

- Avançado

Esta guia compreende as seguintes seções:

- **Registro de aplicativos**. Nesta seção, é possível exibir o registro de aplicativos instalados no dispositivo clientes e suas atualizações, assim como configurar a exibição do registro de aplicativos.

  Informações sobre os aplicativos instalados são fornecidas se o Agente de Rede instalado no dispositivo cliente enviar as informações necessárias ao Servidor de Administração. Você pode configurar o envio de informações para o Servidor de Administração na janela Propriedades do Agente de Rede ou sua política, na seção **Repositórios**.

  Clicar no nome de um aplicativo abre uma janela que contém os detalhes do aplicativo e uma lista dos pacotes de atualização instalados para o aplicativo.

- **Arquivos executáveis**. Esta seção exibe os arquivos executáveis encontrados no dispositivo cliente.

- **Pontos de distribuição**. Esta seção fornece uma lista de pontos de distribuição com os quais o dispositivo interage.

  - Exportar para arquivo

    Clique no botão **Exportar para arquivo** para salvar a um arquivo de uma lista de pontos de distribuição com os quais o dispositivo interage. Por padrão, o aplicativo exporta a lista de dispositivos para um arquivo CSV.

  - Propriedades

    Clique no botão **Propriedades** para exibir e configurar o ponto de distribuição com o qual o dispositivo interage.

- **Registro de hardware**. Nesta seção, é possível visualizar as informações sobre o hardware instalado no dispositivo cliente.

- **Atualizações disponíveis**. Esta seção exibe uma lista de atualizações de software encontradas neste dispositivo, mas ainda não instaladas.

- **Vulnerabilidades de software**. Esta seção fornece informações sobre as vulnerabilidades de aplicativos de terceiros instalados nos dispositivos cliente.

  Para salvar as vulnerabilidades em um arquivo, marque as caixas de seleção ao lado das vulnerabilidades que deseja salvar e clique no botão **Exportar para CSV** ou no botão **Exportar para TXT**.

  Esta seção contém as seguintes configurações:

  - Exibir somente vulnerabilidades que podem ser corrigidas

    Se esta opção estiver ativada, a seção exibe vulnerabilidades que podem ser corrigidas usando um patch.

    Se essa opção estiver desativada, a seção exibe ambas as vulnerabilidades que podem ser corrigidas usando um patch, bem como as vulnerabilidades para as quais não foi lançado nenhum patch.

    Por padrão, esta opção está ativada.

  - Propriedades de vulnerabilidade

Clique no nome de uma vulnerabilidade de software na lista para visualizar as propriedades da vulnerabilidade de software selecionada em uma janela separada. Na janela, você pode fazer o seguinte:

- Ignore a vulnerabilidade de software neste dispositivo gerenciado (no Console de Administração ou no Kaspersky Security Center Cloud Console).
- Consulte a lista de correções recomendadas para a vulnerabilidade.
- Especifique manualmente as atualizações de software para corrigir a vulnerabilidade (no Console de Administração ou no Kaspersky Security Center Cloud Console).
- Exibir as instâncias de vulnerabilidade.
- Consulte a lista de tarefas existentes para corrigir a vulnerabilidade e crie novas tarefas para corrigir a vulnerabilidade.

- **Diagnóstico remoto**. Nesta seção, é possível executar o diagnóstico remoto de dispositivos clientes.

Seleções de dispositivos

As *Seleções de dispositivos* são uma ferramenta para filtrar dispositivos de acordo com as condições específicas. É possível usar as seleções de dispositivos para gerenciar vários dispositivos: por exemplo, para visualizar um relatório apenas sobre esses dispositivos ou mover todos esses dispositivos para outro grupo.

O Kaspersky Security Center Cloud Console fornece uma ampla variedade de *seleções predefinidas* (por exemplo, **Dispositivos com status Crítico**, **A proteção está desativada**, **Foram detectadas ameaças ativas**). As seleções predefinidas não podem ser excluídas. Também é possível criar e configurar *seleções definidas pelos usuários* adicionais.

Em seleções definidas pelos usuários, você pode definir o escopo da pesquisa e selecionar todos os dispositivos, dispositivos gerenciados ou dispositivos não atribuídos. Os parâmetros de pesquisa são especificados nas condições. Na seleção de dispositivos, você pode criar várias condições com parâmetros de pesquisa diferentes. Por exemplo, você pode criar duas condições e especificar conjuntos de IPs diferentes em cada uma delas. Se várias condições forem especificadas, uma seleção exibirá os dispositivos que atendem a alguma das condições. Por outro lado, os parâmetros de pesquisa dentro de uma condição são sobrepostos. Se um conjunto de IPs e o nome de um aplicativo instalado forem especificados em uma condição, apenas esses dispositivos serão exibidos onde o aplicativo está instalado e o endereço IP pertence ao conjunto especificado.

Visualização da lista de dispositivos a partir de uma seleção de dispositivos

O Kaspersky Security Center Cloud Console permite exibir a lista de dispositivos a partir de uma seleção de dispositivos.

Para visualizar a lista de dispositivos na seleção de dispositivos:

1. No menu principal, vá para a seção **Ativos (dispositivos)** → **Seleções de dispositivos** ou **Descoberta e implementação** → **Seleções de dispositivos**.
2. Na lista de seleção, clique no nome da seleção de dispositivos.

A página exibe uma tabela com informações sobre os dispositivos incluídos na seleção de dispositivos.

3. É possível agrupar e filtrar os dados da tabela do dispositivo da seguinte forma:

   - Clique no ícone de configurações ( ) e, em seguida, selecione as colunas a serem exibidas na tabela.
   - Clique no ícone de filtro ( ), especifique e aplique o critério de filtro no menu resultante.

     A tabela filtrada de dispositivos é exibida.

É possível selecionar um ou vários dispositivos na seleção de dispositivos e clicar no botão **Nova tarefa** para criar uma tarefa que será aplicada a esses dispositivos.

Para mover os dispositivos selecionados da seleção de dispositivos para outro grupo de administração, clique no botão **Migrar para grupo** e, em seguida, selecione o grupo de administração de destino.

Criar uma seleção de dispositivos

Para criar uma seleção de dispositivos:

1. No menu principal, vá para **Ativos (dispositivos)** → **Seleções de dispositivos**.

   Uma página com uma lista de seleções de dispositivos é exibida.

2. Clique no botão **Adicionar**.

   A janela **Configurações de seleção de dispositivos** se abre.

3. Digite o nome da nova seleção.

4. Especifique o grupo que contém os dispositivos a serem incluídos na seleção de dispositivos:

   - **Localizar qualquer dispositivo** – Procura dispositivos que atendam aos critérios de seleção e incluídos no grupo **Dispositivos gerenciados** ou **Dispositivos não atribuídos**.
   - **Localizar dispositivos gerenciados** – Procura dispositivos que atendam aos critérios de seleção e incluídos no grupo **Dispositivos gerenciados**.
   - **Localizar dispositivos não atribuídos** – Procura dispositivos que atendam aos critérios de seleção e incluídos no grupo **Dispositivos não atribuídos**.

   É possível ativar a caixa de seleção **Incluir dados dos Servidores de Administração secundários** para ativar a pesquisa de dispositivos que atendam aos critérios de seleção e gerenciados por Servidores de Administração secundários.

5. Clique no botão **Adicionar**.

6. Na janela aberta, especifique as condições que devem ser atendidas para a inclusão de dispositivos nesta seleção e depois clique no botão **OK**.

7. Clique no botão **Salvar**.

A seleção de dispositivos é criada e adicionada à lista de seleções de dispositivos.

Configurar uma seleção de dispositivos

Para configurar uma seleção de dispositivo:

1. No menu principal, vá para **Ativos (dispositivos)** → **Seleções de dispositivos**.

   Uma página com uma lista de seleções de dispositivos é exibida.

2. Escolha a seleção de dispositivos definida pelo usuário relevante e clique no botão **Propriedades**.

   A janela **Configurações de seleção de dispositivos** se abre.

3. Na guia **Geral**, clique no link **Nova condição**.

4. Especifique as condições que devem ser atendidas para a inclusão de dispositivos nesta seleção.

5. Clique no botão **Salvar**.

   As configurações são aplicadas e salvas.

Abaixo estão as descrições das condições para atribuir dispositivos a uma seleção. As condições são combinadas através da utilização do operador lógico OR: a seleção conterá dispositivos que estejam em conformidade com pelo menos uma das condições listadas.

Geral

Na seção **Geral**, você pode mudar o nome de uma condição de seleção e especificar se essa condição deve ser invertida:

Inverter condição de seleção

Se esta opção estiver ativada, a condição de seleção especificada será invertida. A seleção incluirá todos os dispositivos que não atendem a condição.

Por padrão, esta opção está desativada.

Infraestrutura de rede

Na subseção **Rede**, é possível especificar o critério que será usado para incluir dispositivos na seleção de acordo com seus dados na rede:

- Nome do dispositivo

  Nome da rede Windows (nome NetBIOS) do dispositivo ou o endereço IPv4 ou IPv6.

- Domínio

  Exibe todos os dispositivos incluídos no domínio do Windows especificado.

- Grupo de administração

  Exibe os dispositivos incluídos no grupo de administração especificado.

- Descrição

  Texto na janela Propriedades do dispositivo: no campo **Descrição** da seção **Geral**.

  Para descrever texto no campo **Descrição**, é possível usar os seguintes caracteres:

  - Em uma palavra:

    - *. Substitui qualquer sequência por qualquer número de caracteres.

    Exemplo:

    Para descrever as palavras **Servidor** ou **Servidores**, é possível inserir **Servidor***.

    - **?.** Substitui qualquer caractere único.

    Exemplo:

    Para descrever palavras como **Janela** ou **Janelas**, você pode inserir **Janel?.**

    O asterisco (*) ou o ponto de interrogação (**?**) não pode ser usado como o primeiro caractere na consulta.

  - Para encontrar várias palavras:

    - Espaço. Exibe todos os dispositivos cujas descrições contêm qualquer uma das palavras listadas.

    Exemplo:

    Para localizar uma frase que contenha as palavras **Secundário** ou **Virtual**, você pode incluir a linha **Secundário Virtual** na consulta.

    - **+**. Quando o sinal de mais antecede uma palavra, todos os resultados de pesquisa contêm essa palavra.

    Exemplo:

    Para encontrar uma frase que contenha as palavras **Secundário** e **Virtual**, insira **+Secundário+Virtual** na consulta.

    - **-**. Quando um sinal de menos antecede uma palavra, nenhum dos resultados de pesquisa contém essa palavra.

    Exemplo:

    Para encontrar uma frase que contenha **Secundário**, mas que não contenha **Virtual**, insira **+Secundário-Virtual** na consulta.

    - **"<algum texto>"**. O texto dentro de aspas deve estar no texto.

    Exemplo:

    Para encontrar uma expressão que contenha a combinação de palavras **Servidor Secundário**, você pode inserir **"Servidor Secundário"** na consulta.

- Intervalo de IPs

  Se esta opção estiver ativada, você poderá inserir os endereços IP inicial e final do conjunto de IPs no qual os dispositivos relevantes devem ser incluídos.

  Por padrão, esta opção está desativada.

- Gerenciado por outro Servidor de Administração

  Selecione um dos seguintes valores:

  - **Sim**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente gerenciados por outros Servidores de Administração. Esses servidores são diferentes do servidor no qual a regra de migração de dispositivo é configurada.
  - **Não**. A regra de movimentação de dispositivos aplica-se apenas a dispositivos clientes gerenciados pelo Servidor de Administração atual.
  - **Nenhum valor está selecionado**. A condição não se aplica.

Na subseção **Active Directory**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com os dados do Active Directory:

- O dispositivo está em uma unidade organizacional do Active Directory

  Se esta opção estiver ativada, a seleção inclui os dispositivos da unidade organizacional do Active Directory especificada no campo de entrada.

  Por padrão, esta opção está desativada.

- Incluir unidades organizacionais secundárias

  Caso esta opção esteja ativada, a seleção incluirá os dispositivos das unidades de organização secundárias da unidade organizacional do Active Directory especificada.

  Por padrão, esta opção está desativada.

- Este dispositivo é membro de um grupo do Active Directory

  Se esta opção estiver ativada, a seleção incluirá os dispositivos do grupo do Active Directory especificado no campo de entrada.

  Por padrão, esta opção está desativada.

Na subseção **Atividade de rede**, é possível especificar o critério que será usado para incluir dispositivos na seleção de acordo com a sua atividade de rede:

- Atua como ponto de distribuição

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. A seleção inclui dispositivos que agem como pontos de distribuição.
  - **Não**. Dispositivos que atuam como pontos de distribuição não serão incluídos na seleção.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Não desconectar do Servidor de Administração

Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

- **Ativado**. A seleção incluirá dispositivos nos quais a caixa de seleção **Não desconectar do Servidor de Administração** está selecionada.
- **Desativado**. A seleção incluirá dispositivos nos quais a caixa de seleção **Não desconectar do Servidor de Administração** não está selecionada.
- **Nenhum valor está selecionado**. O critério não será aplicado.

- Perfil de conexão trocado

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. A seleção incluirá os dispositivos que se conectaram ao Servidor de Administração após o perfil de conexão ter sido alternado.
  - **Não**. A seleção não incluirá os dispositivos que se conectaram com o Servidor de Administração após o perfil de conexão ter sido alternado.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Última conexão com o Servidor de Administração

  Você pode usar essa caixa de seleção para configurar um critério para pesquisar por dispositivos pela hora da sua última conexão com o Servidor de Administração.

  Se essa caixa de seleção estiver selecionada, é possível, nos campos de entrada especificar o intervalo de tempo (data e hora) durante o qual a última conexão entre o Agente de Rede instalado no dispositivo cliente e o Servidor de Administração foi estabelecida. A seleção inclui dispositivos que estejam no intervalo especificado.

  Se essa caixa de seleção for desmarcada, o critério não é aplicado.

  Por padrão, esta caixa de seleção está desmarcada.

- Novos dispositivos detectados pela sondagem da rede

  Procura por novos dispositivos que tenham sido detectados pela sondagem da rede ao longo dos poucos últimos dias.

  Se esta opção estiver ativada, a seleção somente inclui novos dispositivos que tenham sido detectados pela descoberta de dispositivos durante a quantidade de dias especificada no campo **Período de detecção (dias)**.

  Se esta opção estiver ativada, a seleção inclui todos os dispositivos que tenham sido detectados pela descoberta de dispositivos.

  Por padrão, esta opção está desativada.

- Dispositivo visível

Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

- **Sim**. O aplicativo é incluído na seleção de dispositivos atualmente visíveis na rede.
- **Não**. O aplicativo é incluído na seleção de dispositivos atualmente invisíveis na rede.
- **Nenhum valor está selecionado**. O critério não será aplicado.

Na subseção **Segmentos da nuvem**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com os seus respectivos segmentos da nuvem:

- O dispositivo está no segmento da nuvem

  Caso a opção esteja ativada, será possível escolher os dispositivos dos segmentos da nuvem AWS, Azure e Google.

  Caso a opção **Incluir objetos secundários** esteja marcada, a pesquisa será executada em todos os objetos secundários do segmento especificado.

  Os resultados da pesquisa somente incluem dispositivos do segmento selecionado.

- Dispositivo detectado usando a API

  Na lista suspensa, você pode selecionar se um dispositivo é detectado pelas ferramentas API:

  - **Sim**. O dispositivo é detectado usando a API da AWS, Azure ou Google.
  - **Não**. O dispositivo não pode ser detectado usando a API da AWS, do Azure ou do Google. Ou seja, o dispositivo está fora do ambiente de nuvem ou está no ambiente em nuvem, mas não pode ser detectado usando uma API.
  - Nenhum valor. Esta condição não se aplica.

Status do dispositivo

Na seção **Status do dispositivo gerenciado**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com a descrição do status de dispositivos de um aplicativo gerenciado:

- Status do dispositivo

  Lista suspensa na qual você pode selecionar um dos status do dispositivo: *OK*, *Crítico* ou *Advertência*.

- Status da proteção em tempo real

  Lista suspensa na qual você pode selecionar o status da proteção em tempo real. Os dispositivos com um status da proteção em tempo real especificado serão incluídos na seleção.

- Descrição do status do dispositivo

Neste campo, você poderá selecionar caixas de seleção próximas das condições que, se atendidas, atribuem um dos seguintes status ao dispositivo: *OK, Crítico* ou *Advertência*.

Na subseção **Status dos componentes em aplicativos gerenciados**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o status dos componentes em aplicativos gerenciados:

- **Status da prevenção de vazamento de dados**

  Pesquise dispositivos pelo status da Prevenção de vazamento de dados (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

- **Status da proteção dos servidores de colaboração**

  Procure dispositivos pelo status da proteção de colaboração do servidor (*Sem dados do dispositivo*, *Parado*, *Iniciando, Pausado*, *Executando*, *Falhou*).

- **Status da proteção antivírus dos servidores de correio**

  Procure dispositivos pelo status da proteção do servidor de e-mail (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

- **Status do Endpoints Sensor**

  Procure dispositivos pelo status do componente Endpoint Sensor (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

Na subseção **Problemas que afetam o status em aplicativos gerenciados**, é possível especificar os critérios que serão usados para incluir os dispositivos na seleção de acordo com a lista de possíveis problemas detectados por um aplicativo gerenciado. Se pelo menos um problema que você selecionar existir em um dispositivo, o dispositivo estará incluído na seleção. Quando você seleciona um problema listado para vários aplicativos, você tem a opção de selecionar esse problema em todas das listas automaticamente.

Você pode selecionar as caixas de seleção para descrições de status do aplicativo gerenciado; ao receber este status, os dispositivos serão incluídos na seleção. Quando você seleciona um status listado para vários aplicativos, você tem a opção de selecionar esse status em todas das listas automaticamente.

Detalhes do sistema

Na seção **Sistema operacional**, você pode especificar o critério que será usado para incluir dispositivos na seleção de acordo com o seu tipo de sistema operacional.

- **Tipo de plataforma**

  Se esta caixa de seleção estiver marcada, você pode selecionar um sistema operacional da lista. Os dispositivos com o sistema operacional especificado instalado são incluídos nos resultados de pesquisa.

- **Versão do service pack do sistema operacional**

Nesse campo, é possível especificar a versão do pacote do sistema operacional (no formato *X.Y*), que determinará como a regra para mover será aplicada ao dispositivo. Por padrão, nenhum valor de versão é especificado.

- Tipo de bit do sistema operacional

  Na lista suspensa, você poderá selecionar a arquitetura para o sistema operacional, que determinará como a regra para mover será aplicada ao dispositivo (**Desconhecido**, **x86**, **AMD64** ou **IA64**). Por padrão, nenhuma opção é selecionada na lista para que a arquitetura do sistema operacional não fique definida.

- Compilação do sistema operacional

  Esta configuração é aplicável somente aos sistemas operacionais Windows.

  O número da compilação do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um número de compilação igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de compilação, exceto o especificado.

- Número da versão do sistema operacional

  Esta configuração é aplicável somente aos sistemas operacionais Windows.

  O identificador (ID) da versão do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um ID da versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de ID da versão, exceto o especificado.

Na seção **Máquinas virtuais**, você pode definir o critério para incluir os dispositivos na seleção se estes são máquinas virtuais ou parte da Virtual Desktop Infrastructure (VDI):

- Esta é uma máquina virtual

  Na lista suspensa, você pode selecionar as seguintes opções:

  - **Indefinido**.
  - **Não**. Localizar dispositivos que não sejam máquinas virtuais.
  - **Sim**. Localizar dispositivos que são máquinas virtuais.

- Tipo de máquina virtual

  Na lista suspensa, você pode selecionar o fabricante da máquina virtual.

  Essa lista suspensa estará disponível se o valor **Sim** ou **Irrelevante** estiver selecionado na lista suspensa **Esta é uma máquina virtual**.

- Parte da Virtual Desktop Infrastructure

Na lista suspensa, você pode selecionar as seguintes opções:

- **Indefinido**.
- **Não**. Localizar dispositivos que não fazem parte da Virtual Desktop Infrastructure.
- **Sim**. Localizar dispositivos que fazem parte da Virtual Desktop Infrastructure (VDI).

Na subseção **Registro de hardware**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o hardware instalado:

Verifique e confirme se o utilitário lshw está instalado nos dispositivos Linux a partir dos quais deseja buscar detalhes de hardware. Os detalhes de hardware obtidos de máquinas virtuais podem estar incompletos, dependendo do hipervisor usado.

- Dispositivo

  Na lista suspensa, você pode selecionar um tipo de unidade. Todos os dispositivos com esta unidade são incluídos nos resultados da pesquisa.

  O campo suporta a pesquisa de texto completo.

- Fornecedor

  Na lista suspensa, você pode selecionar o nome do fabricante da unidade. Todos os dispositivos com esta unidade são incluídos nos resultados da pesquisa.

  O campo suporta a pesquisa de texto completo.

- Nome do dispositivo

  Nome do dispositivo na rede Windows. O dispositivo com o nome especificado será incluído na seleção.

- Descrição

  Descrição de um dispositivo ou de uma unidade de hardware. Os dispositivos com a descrição especificada neste campo serão incluídos na seleção.

  A descrição de um dispositivo em qualquer formado pode ser inserida na janela de propriedades desse dispositivo. O campo suporta a pesquisa de texto completo.

- Fornecedor do dispositivo

  Nome do fabricante do dispositivo. Os dispositivos produzidos pelo fabricante especificado neste campo estão incluídos na seleção.

  Você pode inserir o nome do fabricante na janela de propriedades de um dispositivo.

- Número de série

  Todas as unidades hardware com número de série especificado nesse campo serão incluídas na seleção.

- **Número de inventário**

  Equipamentos com o número de inventário especificado neste campo serão incluídos na seleção.

- **Usuário**

  Todas as unidades hardware do usuário especificado nesse campo serão incluídas na seleção.

- **Localização**

  A localização do dispositivo ou unidade de hardware (por exemplo, na sede ou no escritório de uma filial). Computadores ou outros dispositivos que são implementados na localização especificada nesse campo serão incluídos na seleção.

  Você pode descrever a localização de um dispositivo em qualquer formato na janela de propriedades desse dispositivo.

- **Frequência do clock da CPU em MHz, de**

  A taxa de clock mínima de uma CPU. Os dispositivos com uma CPU que corresponda ao intervalo de taxa de clock especificado nos campos de entrada (inclusive) serão incluídos na seleção.

- **Frequência do clock da CPU em MHz, para**

  A taxa de clock máxima de uma CPU. Os dispositivos com uma CPU que corresponda ao intervalo de taxa de clock especificado nos campos de entrada (inclusive) serão incluídos na seleção.

- **Número de núcleos da CPU virtual, de**

  O número mínimo de núcleos de CPU virtuais. Os dispositivos com uma CPU que corresponda ao intervalo do número de núcleos virtuais especificado nos campos de entrada (inclusive) serão incluídos na seleção.

- **Número de núcleos da CPU virtual, até**

  O número máximo de núcleos de CPU virtuais. Os dispositivos com uma CPU que corresponda ao intervalo do número de núcleos virtuais especificado nos campos de entrada (inclusive) serão incluídos na seleção.

- **Volume do disco rígido, em GB, de**

  O volume mínimo do disco rígido no dispositivo. Os dispositivos com um disco rígido que corresponda a faixa especificada nos campos de entrada (inclusive) serão incluídos na seleção.

- **Volume do disco rígido, em GB, para**

  O volume máximo do disco rígido no dispositivo. Os dispositivos com um disco rígido que corresponda a faixa especificada nos campos de entrada (inclusive) serão incluídos na seleção.

- **Tamanho da RAM em MB, de**

O tamanho mínimo da RAM do dispositivo. Os dispositivos com RAM que corresponda ao intervalo de tamanho especificado nos campos de entrada (inclusive) serão incluídos na seleção.

- Tamanho da RAM em MB, para

  O tamanho máximo da RAM do dispositivo. Os dispositivos com RAM que corresponda ao intervalo de tamanho especificado nos campos de entrada (inclusive) serão incluídos na seleção.

Detalhes de software de terceiros

Na subseção **Registro de aplicativos**, é possível definir o critério para pesquisar dispositivos de acordo com os aplicativos neles instalados:

- Nome do aplicativo

  Lista suspensa na qual é possível selecionar um aplicativo. Os dispositivo nos quais o aplicativos especificado estiver instalado, serão incluídos na seleção.

- Versão do aplicativo

  Campo de entrada onde é possível especificar a versão do aplicativo selecionado.

- Fornecedor

  Lista suspensa na qual é possível selecionar o fabricante de um aplicativo instalado no dispositivo.

- Status do aplicativo

  Uma lista suspensa na qual é possível selecionar o status de um aplicativo (*Instalado*, *Não instalado*). Os dispositivos nos quais o aplicativo especificado está ou não instalado, dependendo do status selecionado, serão incluídos na seleção.

- Localizar por atualização

  Se esta opção estiver ativada, a pesquisa será executada usando os dados das atualizações para os aplicativos instalados nos dispositivos relevantes. Após selecionar a caixa de seleção, os campos **Nome do aplicativo**, **Versão do aplicativo** e **Status do aplicativo** mudam para **Nome da atualização**, **Versão da atualização** e **Status** respectivamente.

  Por padrão, esta opção está desativada.

- Nome do aplicativo de segurança incompatível

  Lista suspensa na qual é possível selecionar aplicativos de segurança de terceiros. Durante a pesquisa, os dispositivos nos quais está instalado o aplicativo especificado, serão incluídos na seleção.

- Tag do aplicativo

Na lista suspensa, você pode selecionar a tag do aplicativo. Todos os dispositivos que instalaram aplicativos com a tag selecionada na descrição são incluídos na seleção de dispositivo.

- Aplicar aos dispositivos sem tags especificadas

  Se esta opção estiver ativada, o perfil da política inclui dispositivos com descrições que não contêm nenhuma das tags selecionadas.

  Se esta opção estiver desativada, o critério não é aplicado.

  Por padrão, esta opção está desativada.

Na subseção **Vulnerabilidades e atualizações**, é possível especificar o critério que será usado para incluir dispositivos na seleção de acordo com a fonte do Windows Update:

WUA foi mudado para o Servidor de Administração

Você pode selecionar uma das seguintes opções de pesquisa da lista suspensa:

- **Sim**. Se essa opção estiver selecionada, os resultados da pesquisa incluirão os dispositivos que recebem atualizações através do Windows Update do Servidor de Administração.
- **Não**. Caso essa opção esteja selecionada, os resultados incluirão os dispositivos que recebem atualizações pelo Windows Update de outras fontes.

Detalhes de aplicativos Kaspersky

Na subseção **Aplicativos Kaspersky**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o aplicativo gerenciado selecionado:

- Nome do aplicativo

  Na lista suspensa, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo nome de um aplicativo da Kaspersky.

  A lista somente fornece os nomes de aplicativos com plugins de gerenciamento instalados na estação de trabalho do administrador.

  Se nenhum aplicativo for selecionado, o critério não será aplicado.

- Versão do aplicativo

  No campo de entrada, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo número da versão de um aplicativo da Kaspersky.

  Se nenhum número de versão for especificado, o critério não será aplicado.

- Nome da atualização crítica

  Uma lista suspensa na qual é possível selecionar o status de um aplicativo (*Instalado*, *Não instalado*). Os dispositivos nos quais o aplicativo especificado está ou não instalado, dependendo do status selecionado, serão incluídos na seleção.

No campo de entrada de dados, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo nome do aplicativo ou pelo número do pacote de atualização.

Se o campo for deixado em branco, o critério não será aplicado.

- Selecione o período da última atualização de módulos

  Você pode usar esta opção para definir um critério para pesquisar dispositivos pela hora da última atualização dos módulos de aplicativos instalados nesses dispositivos.

  Se essa caixa de seleção estiver selecionada, nos campos de entrada você poderá especificar o intervalo de tempo (data e hora) durante o qual a última atualização de módulos de aplicativos instalados nesses dispositivos foi executada.

  Se essa caixa de seleção for desmarcada, o critério não é aplicado.

  Por padrão, esta caixa de seleção está desmarcada.

- O dispositivo é gerenciado pelo Servidor de Administração

  Na lista suspensa, é possível incluir na seleção os dispositivos gerenciados pelo Kaspersky Security Center Cloud Console:

  - **Sim**. O aplicativo inclui a seleção de dispositivos gerenciados pelo Kaspersky Security Center Cloud Console.
  - **Não**. O aplicativo inclui na seleção os dispositivos que não são gerenciados pelo Kaspersky Security Center Cloud Console.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Aplicativo de segurança instalado

  Na lista suspensa, você poderá incluir na seleção todos os dispositivos com o aplicativo de segurança instalado:

  - **Sim**. O aplicativo é incluído na seleção de dispositivos com o aplicativo de segurança instalado.
  - **Não**. O aplicativo inclui na seleção todos os dispositivos sem nenhum aplicativo de segurança instalado.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

Na subseção **Proteção antivírus**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o status da proteção:

- Bancos de dados lançados

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes por data de lançamento de versão do banco de dados antivírus. Nos campos de entrada, você pode definir o intervalo de tempo com base no qual a pesquisa é realizada.

  Por padrão, esta opção está desativada.

- Contagem de registros do banco de dados

Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pelo número de registros de banco de dados. Nos campos de entrada, você pode definir os valores do limite inferior e superior para os registros do banco de dados antivírus.

Por padrão, esta opção está desativada.

- Última verificação

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pela hora da última verificação de malwares. No campo de entrada, você poderá especificar o período de tempo no qual a última verificação de malwares foi executada.

  Por padrão, esta opção está desativada.

- Ameaças detectadas

  Algoritmo de criptografia de bloco simétrico Advanced Encryption Standard (AES). Na lista suspensa, você pode selecionar o tamanho de chave de criptografia (de 56 bits, de 128 bits, de 192 bits ou de 256 bits).

  Valores disponíveis: *AES56*, *AES128*, *AES192* e *AES256*.

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pelo número de vírus detectados. Nos campos de entrada, você pode definir os valores limite inferiores e superiores pelo número de vírus encontrados.

  Por padrão, esta opção está desativada.

A subseção **Componentes do aplicativo** contém a lista de componentes desses aplicativos que têm plug-ins de gerenciamento correspondentes instalados no Kaspersky Security Center Cloud Console.

Na subseção **Componentes do aplicativo**, é possível especificar o critério para a inclusão de dispositivos em uma seleção de acordo com o status e os números da versão dos componentes que fazem referência ao aplicativo que for selecionado:

- Status

Pesquise dispositivos segundo o status do componente enviado por um aplicativo ao Servidor de Administração. É possível selecionar um dos seguintes status: *N/A, Interrompido*, *Pausado*, *Iniciando*, *Em execução, Com falha*, *Não instalado, Não compatível com a licença*. Se o componente selecionado do aplicativo instalado em um dispositivo gerenciado tiver o status especificado, o dispositivo será incluído na seleção de dispositivos.

Status enviados pelos aplicativos:

- *Interrompido* – O componente está desativado e não está funcionando no momento atual.
- *Pausado* – O componente está suspenso, por exemplo, depois que o usuário pausou a proteção no aplicativo gerenciado.
- *Iniciando* – O componente está atualmente em processo de inicialização.
- *Executando* – O componente está ativado e funcionando corretamente.
- *Falha* – Um erro ocorreu durante a operação do componente.
- *Não instalado* – O usuário não selecionou o componente para instalação ao configurar a instalação personalizada do aplicativo.
- *Não compatível com a licença* – A licença não cobre o componente selecionado.

Diferentemente de outros status, o status *N/A* não é enviado pelos aplicativos. Esta opção mostra que os aplicativos não têm nenhuma informação sobre o status do componente selecionado. Por exemplo, isto pode acontecer quando o componente selecionado não pertence a nenhum dos aplicativos instalados no dispositivo, ou quando o dispositivo está desligado.

- **Versão**

Pesquise dispositivos segundo o número da versão do componente que você selecionar na lista. Você pode digitar um número de versão, por exemplo `3.4.1.0`, e especificar se o componente selecionado deve ter uma versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todas as versões, exceto a especificada.

Tags

Na seção **Tags**, você pode configurar o critério para pesquisar por dispositivos com base em palavras-chave (tags) adicionadas anteriormente às descrições dos dispositivos gerenciados:

Aplicar se pelo menos uma tag especificada corresponder

Se esta opção estiver ativada, o resultado da pesquisa mostrará os dispositivos com descrições que contêm ao menos uma das tags selecionadas.

Se esta opção estiver ativada, o resultado da pesquisa irá mostrar os dispositivos com descrições que não contêm todos as tags selecionadas.

Por padrão, esta opção está desativada.

Para adicionar tags ao critério, clique no botão **Adicionar** e selecione as tags clicando no campo de entrada **Tag**. Especifique se deseja incluir ou excluir os dispositivos com as tags selecionadas na seleção de dispositivos.

- **Deve ser incluído**

  Se esta opção for selecionada, os resultados da pesquisa exibirão os dispositivos cujas descrições contêm a tag selecionada. Para encontrar dispositivos, você pode usar o asterisco, que indica qualquer sequência de caracteres com qualquer número de caracteres.

  Por padrão, esta opção está selecionada.

- **Deve ser excluído**

  Se esta opção for selecionada, os resultados da pesquisa exibirão os dispositivos cujas descrições não contêm a tag selecionada. Para encontrar dispositivos, você pode usar o asterisco, que indica qualquer sequência de caracteres com qualquer número de caracteres.

Usuários

Na seção **Usuários**, você pode definir o critério para incluir dispositivos na seleção de acordo com as contas de usuários que efetuaram o login no sistema operacional.

- **Último usuário que fez login no sistema**

  Se a opção estiver ativada, será possível selecionar a conta de usuário para configurar o critério. Observe que a lista de usuários é filtrada e exibe os usuários internos. Os resultados da pesquisa incluirão os dispositivos nos quais o usuário selecionado efetuou o último login no sistema.

- **Usuário que fez login no sistema pelo menos uma vez**

  Se a opção estiver ativada, será possível selecionar a conta de usuário para configurar o critério. Observe que a lista de usuários é filtrada e exibe os usuários internos. Os resultados da pesquisa incluirão os dispositivos nos quais o usuário especificado efetuou o login no sistema ao menos uma vez.

Exportação da lista de dispositivos a partir de uma seleção de dispositivos

O Kaspersky Security Center Cloud Console permite salvar informações sobre dispositivos a partir de uma seleção de dispositivos e exportá-las para um arquivo CSV ou TXT.

Para exportar a lista de dispositivos na seleção de dispositivos:

1. Abra a tabela com os dispositivos a partir da seleção de dispositivos.
2. Use uma das seguintes formas para selecionar os dispositivos que deseja exportar:
   - Para selecionar dispositivos específicos, marque as caixas de seleção ao lado deles.
   - Para selecionar todos os dispositivos da página da tabela atual, marque a caixa de seleção no cabeçalho da tabela de dispositivos e, em seguida, marque a caixa de seleção **Selecionar tudo na página atual**.
   - Para selecionar todos os dispositivos da tabela, marque a caixa de seleção no cabeçalho da tabela de dispositivos e, em seguida, marque a caixa de seleção **Selecionar tudo**.

Clique no botão **Exportar para CSV** ou **Exportar para TXT**. Todas as informações sobre os dispositivos selecionados incluídos na tabela serão exportadas.

Observe que, caso um critério de filtro tenha sido aplicado na tabela de dispositivos, apenas os dados filtrados das colunas exibidas serão exportados.

Remover os dispositivos de grupos de administração em uma seleção

Ao trabalhar com uma seleção de dispositivos, você poderá remigrar dispositivos dos grupos de administração diretamente nesta seleção, sem alternar para os grupos de administração dos quais estes dispositivos precisam ser removidos.

Para remigrar dispositivos de grupos de administração:

1. No menu principal, vá para **Ativos (dispositivos)** → **Seleções de dispositivos** ou **Descoberta e implementação** → **Seleções de dispositivos**.
2. Na lista de seleção, clique no nome da seleção de dispositivos.

   A página exibe uma tabela com informações sobre os dispositivos incluídos na seleção de dispositivos.
3. Selecione os dispositivos que deseja remover e, em seguida, clique em **Excluir**.

   Os dispositivos selecionados serão removidos de seus respectivos grupos de administração.

Exibir e configurar as ações quando os dispositivos mostram inatividade

Se os dispositivos cliente em um grupo estiverem inativos, você poderá receber notificações sobre isso. Você também pode excluir automaticamente esses dispositivos.

Para exibir ou configurar as ações quando os dispositivos no grupo mostrarem inatividade:

1. No menu principal, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Clique no nome do grupo de administração necessário.

   A janela Propriedades do grupo de administração é aberta.
3. Na janela Propriedades, siga para a guia **Configurações**.
4. Na seção **Herança**, ative ou desative as seguintes opções:

   - Herdar do grupo principal

     As configurações desta seção serão herdadas do grupo principal no qual o dispositivo cliente está incluído. Se esta opção estiver ativada, as configurações sob **Atividade de dispositivos na rede** serão bloqueadas contra quaisquer alterações.

     Esta opção está disponível somente se o grupo de administração tiver um grupo principal.

     Por padrão, esta opção está ativada.

- Forçar herança de configurações nos grupos secundários

  Os valores de configuração serão distribuídos aos grupos secundários, mas essas configurações são bloqueadas nas propriedades dos grupos secundários.

  Por padrão, esta opção está desativada.

5. Na seção **Atividade de dispositivos**, ative ou desative as seguintes opções:

   - Notificar o administrador se o dispositivo estiver inativo por mais de (dias)

     Se esta opção estiver ativada, o administrador receberá notificações sobre os dispositivos inativos. Você pode especificar o intervalo de tempo após o qual o evento **O dispositivo permaneceu inativo na rede por muito tempo** será criado. O intervalo de tempo predefinido é de 7 dias.

     Por padrão, esta opção está ativada.

   - Remover o dispositivo do grupo se estiver inativo por mais de (dias)

     Se esta opção estiver selecionada, você poderá especificar o intervalo de tempo após o qual o dispositivo será automaticamente removido do grupo. O intervalo de tempo predefinido é de 60 dias.

     Por padrão, esta opção está ativada.

6. Clique em **Salvar**.

   As suas alterações serão salvas e aplicadas.

Sobre os status do dispositivo

O Kaspersky Security Center Cloud Console atribui um status a cada dispositivo gerenciado. O status específico depende se as condições definidas pelo usuário são atendidas. Em alguns casos, ao atribuir um status a um dispositivo, o Kaspersky Security Center Cloud Console leva em consideração o sinalizador de visibilidade do dispositivo na rede (consulte a tabela abaixo). Se o Kaspersky Security Center Cloud Console não encontrar um dispositivo na rede dentro de duas horas, o sinalizador de visibilidade do dispositivo será definido como *Não visível*.

Os status são os seguintes:

- *Crítico* ou *Crítico/Visível*
- *Advertência* ou *Advertência/Visível*
- *OK* ou *OK/Visível*

A tabela abaixo lista as condições padrão que devem ser atendidas para atribuir o status *Crítico* ou *Advertência* a um dispositivo, com todos os valores possíveis.

Condições para atribuir um status a um dispositivo

Condição	Descrição da condição	Valores disponíveis
O aplicativo de segurança não está instalado	O Agente de Rede é instalado no dispositivo, mas um aplicativo de segurança não é instalado.	• O botão de alternar é

		ativado. • O botão de alternar é desativado.
Excesso de vírus detectados	Alguns vírus foram encontrados no dispositivo por uma tarefa de detecção de vírus, por exemplo, a tarefa de verificação de vírus, e o número de vírus encontrados excede o valor especificado.	Mais de 0.
O nível da proteção em tempo real é diferente do nível definido pelo administrador	O dispositivo está visível na rede, mas o nível de proteção em tempo real difere do nível definido (na condição) pelo administrador para o status do dispositivo.	• Parado. • Pausada. • Executando.
A verificação de malwares não é executada há muito tempo	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas nem a tarefa de *verificação de malware* nem a verificação local foram executadas dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 7 dias ou antes.	Mais de 1 dia.
Os bancos de dados estão desatualizados	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas os bancos de dados antivírus não foram atualizados neste dispositivo dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 1 dia ou antes.	Mais de 1 dia.
Não conectado há muito tempo	O Agente de Rede está instalado no dispositivo, mas o dispositivo não se conectou a um Servidor de Administração dentro do intervalo de tempo especificado, porque o dispositivo estava desativado.	Mais de 1 dia.
Foram detectadas ameaças ativas	O número de objetos não processados na pasta **Ameaças ativas** excede o valor especificado.	Mais de 0 itens.
A reinicialização é necessária	O dispositivo está visível na rede, mas um aplicativo requer o reinício do dispositivo por mais tempo do que o intervalo de tempo especificado e para um dos motivos selecionados.	Mais de 0 minuto.
Aplicativos incompatíveis estão instalados	O dispositivo está visível na rede, mas o inventário de software executado pelo Agente de Rede detectou aplicativos incompatíveis instalados no dispositivo.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Foram detectadas vulnerabilidades de software	O dispositivo está visível na rede, e o Agente de Rede está instalado no dispositivo, mas a tarefa *Encontrar vulnerabilidades e atualizações necessárias* detectou vulnerabilidades com o nível de gravidade especificado nos aplicativos instalados no dispositivo.	• Crítico. • Alto. • Médio.

		• Ignorar se a vulnerabilidade não puder ser corrigida. • Ignorar se uma atualização for atribuída para instalação.
A licença expirou	O dispositivo está visível na rede, mas a licença expirou.	• O botão de alternar é desativado. • O botão de alternar é ativado.
A licença expira em breve	O dispositivo está visível na rede, mas a licença expirará no dispositivo em tempo menor que o número especificado de dias.	Mais de 0 dias.
A verificação de atualizações do Windows Update não é executada há muito tempo	O dispositivo está visível na rede, mas a tarefa Executar a sincronização com o Windows Update não foi executada dentro do intervalo de tempo especificado.	Mais de 1 dia.
Status de criptografia inválido	O Agente de Rede está instalado no dispositivo, mas o resultado da criptografia de dispositivo é igual ao valor especificado.	• Não está em conformidade com a política devido à recusa do usuário (somente para dispositivos externos). • Não está em conformidade com a política devido a um erro. • Reiniciar é necessário ao aplicar a política. • Nenhuma política de criptografia está especificada. • Sem suporte.

		• Ao aplicar a política.
As configurações do dispositivo móvel não estão em conformidade com a política	As configurações do dispositivo móvel são diferentes das especificadas na política do Kaspersky Endpoint Security for Android durante a verificação das regras de conformidade.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Foram detectados problemas de segurança não processados	Alguns problemas de segurança não processados foram encontrados no dispositivo. Os problemas de segurança podem ser criados automaticamente pelos aplicativos da Kaspersky gerenciados e instalados no dispositivo cliente ou manualmente pelo administrador.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Status do dispositivo definido pelo aplicativo	O status do dispositivo é definido pelo aplicativo gerenciado.	• O botão de alternar é desativado. • O botão de alternar é ativado.
O dispositivo está com espaço em disco insuficiente	O espaço livre em disco no dispositivo é menor do que o valor especificado ou o dispositivo não pôde ser sincronizado com o Servidor de Administração. O status *Crítico* ou *Advertência* é alterado para o status *OK* quando o dispositivo é sincronizado com sucesso com o Servidor de Administração, e o espaço livre no dispositivo é maior que ou igual ao valor especificado.	Mais de 0 MB
O dispositivo está sem gerenciamento	Durante a descoberta de dispositivos, o dispositivo foi reconhecido como visível na rede, mas houve falha em mais de três tentativas de sincronizar com o Servidor de Administração.	• O botão de alternar é desativado. • O botão de alternar é ativado.
A proteção está desativada	O dispositivo é visível na rede, mas o aplicativo de segurança no dispositivo foi desativado por um tempo mais longo do que o intervalo de tempo especificado. Nesse caso, o estado do aplicativo de segurança é *interrompido* ou *com falha* e diferente de: *iniciando*, *em execução* ou *suspenso*.	Mais de 0 minuto.
O aplicativo de segurança não está em execução	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas não está em execução.	• O botão de alternar é desativado.

		• O botão de alternar é ativado.

O Kaspersky Security Center Cloud Console permite definir a alternância automática do status de um dispositivo em um grupo de administração quando as condições especificadas forem atendidas. Quando as condições especificadas forem atendidas, ao dispositivo cliente é atribuído um dos seguintes status: *Crítico* ou *Aviso*. Quando as condições especificadas não são atendidas, o dispositivo cliente recebe o status *OK*.

Diferentes status poderão corresponder a diferentes valores de uma condição. Por exemplo, se por padrão a condição **Os bancos de dados estão desatualizados** possuir o valor **Mais de 3 dias**, o dispositivo cliente recebe o status *Advertência*. Se o valor for **Mais de 7 dias**, é atribuído o status *Crítico*.

Quando o Kaspersky Security Center Cloud Console atribui um status a um dispositivo, para algumas condições (consulte a coluna Descrição da condição), o sinalizador de visibilidade é levado em consideração. Por exemplo, se um dispositivo gerenciado recebeu o status *Crítico* porque a condição Os bancos de dados estão desatualizados foi atendida e, mais tarde, o sinalizador de visibilidade foi definido para o dispositivo, então o dispositivo recebe o status *OK*.

Configurar a alternância dos status do dispositivo

Você pode alterar as condições para atribuir o status *Crítico* ou *Advertência* para um dispositivo.

Para ativar a alteração do status do dispositivo para Crítico:

1. No menu principal, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Crítico**.
5. No painel direito, na seção **Se especificados, definir como Crítico**, ative a condição para alterar o status de um dispositivo para *Crítico*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.

9. Clique em **OK**.

Quando condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Crítico*.

Para ativar a alteração do status do dispositivo para Advertência:

1. No menu principal, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Advertência**.
5. No painel direito, na seção **Se especificados, definir como Advertência**, ative a condição para alterar o status de um dispositivo para *Advertência*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.

9. Clique em **OK**.

Quando as condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Advertência*.

Alterar o Servidor de Administração para dispositivos cliente

É possível alterar o Servidor de Administração que gerencia os dispositivos cliente por outro, usando a tarefa **Alterar o Servidor de Administração**. Após a conclusão da tarefa, os dispositivos clientes selecionados serão colocados sob o gerenciamento do Servidor de Administração especificado por você. Você pode alternar o gerenciamento do dispositivo entre os seguintes Servidores de Administração:

- Servidor de Administração principal e um de seus Servidores de Administração virtuais
- Dois Servidores de Administração virtuais do mesmo Servidor de Administração principal

Para alterar o Servidor de Administração que gerencia dispositivos cliente para outro servidor:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Para o aplicativo Kaspersky Security Center Cloud Console, selecione o tipo de tarefa **Alterar o Servidor de Administração**.
4. Especifique o nome da tarefa que está criando.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).

5. Dispositivos aos quais a tarefa será atribuída.

6. Selecione o Servidor de Administração que deseja usar para gerenciar os dispositivos selecionados.

7. Especificar as configurações da conta:

   - **Conta padrão**

     A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

     Por padrão, esta opção está selecionada.

   - **Especificar conta**

     Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

   - **Conta**

     Conta sob a qual a tarefa é executada.

   - **Senha**

     Senha da conta sob a qual a tarefa será executada.

8. Se na página **Concluir a criação da tarefa**, você ativar a opção **Abrir detalhes da tarefa quando a criação for concluída**, você pode modificar as configurações padrão da tarefa. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.

10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

11. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

12. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

13. Execute a tarefa criada.

Após a conclusão da tarefa, os dispositivos cliente, para os quais a mesma foi criada, são colocados sob gerenciamento pelo Servidor de Administração especificado nas configurações da tarefa.

Sobre clusters e matrizes de servidores

O Kaspersky Security Center Cloud Console é compatível com tecnologia de cluster. Se o Agente de Rede enviar uma informação ao Servidor de Administração confirmando que o aplicativo instalado no dispositivo cliente faz parte de uma matriz de servidor, este dispositivo cliente torna-se um nó de cluster.

Caso um grupo de administração contenha clusters ou matrizes de servidor, a página **Dispositivos gerenciados** exibe duas guias – uma para dispositivos individuais e outra para clusters e matrizes de servidor. Depois que os dispositivos gerenciados são detectados como nós de cluster, o cluster é adicionado como um objeto individual à guia **Grupamentos e matrizes de servidores**.

Os nós da matriz de cluster ou servidor são listados na guia **Dispositivos**, juntamente com outros dispositivos gerenciados. É possível ver propriedades dos nós como dispositivos individuais e executar outras operações, mas não é possível excluir um nó de cluster ou movê-lo para outro grupo de administração separadamente de seu cluster. Só é possível excluir ou mover um cluster inteiro.

É possível executar as seguintes operações com clusters ou matrizes de servidor:

- Ver propriedades
- Mover o cluster ou matriz de servidores para outro grupo de administração

  Ao mover um cluster ou matriz de servidores para outro grupo, todos os seus nós são movidos com ele, porque um cluster e qualquer um de seus nós sempre pertencem ao mesmo grupo de administração.

- Excluir

  É razoável excluir um cluster ou matriz de servidor somente quando o cluster ou matriz de servidor não existir mais na rede da organização. Se um cluster ainda estiver visível em sua rede e o Agente de Rede e o aplicativo de segurança Kaspersky ainda estiverem instalados nos nós do cluster, o Kaspersky Security Center Cloud Console retornará automaticamente o cluster excluído e seus nós à lista de dispositivos gerenciados.

Propriedades de um cluster ou matriz de servidores

Para visualizar as configurações de um cluster ou matriz de servidores:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados** → **Grupamentos e matrizes de servidores**.

   A lista de clusters e matrizes de servidores é exibida.

2. Clique no nome do cluster ou matriz de servidor necessária.

A janela de propriedades do cluster ou matriz de servidor selecionada é exibida.

Geral

A seção **Geral** exibe informações gerais sobre o cluster ou a matriz de servidores. As informações são fornecidas com base nos dados recebidos durante a última sincronização dos nós do cluster com o Servidor de Administração:

- **Nome**
- **Descrição**
- **Domínio do Windows**

Domínio ou grupo de trabalho do Windows, que contém o cluster ou a matriz do servidor.

- Nome do NetBIOS

  Nome da rede Windows do cluster ou matriz de servidor.

- Nome DNS

  Nome do domínio DNS do cluster ou matriz de servidor.

Tarefas

Na guia **Tarefas**, é possível gerenciar as tarefas atribuídas ao cluster ou matriz de servidores: visualizar a lista de tarefas existentes; criar novas tarefas; remover, iniciar e interromper tarefas; modificar as suas configurações; e visualizar os resultados da execução. As tarefas listadas estão relacionadas ao aplicativo de segurança Kaspersky instalado nos nós do cluster. O Kaspersky Security Center Cloud Console recebe a lista de tarefas e os detalhes do status da tarefa dos nós do cluster. Se uma conexão não for estabelecida, o status não será exibido.

Nós

Essa guia exibe uma lista de nós incluídos no cluster ou na matriz do servidor. É possível clicar em um nome de nó para visualizar a janela de propriedades do dispositivo.

Aplicativo Kaspersky

A janela de propriedades também pode conter guias adicionais com informações e configurações relacionadas ao aplicativo de segurança Kaspersky instalado nos nós do cluster.

Tags de dispositivo

Esta seção descreve identificadores do dispositivo e fornece instruções para criá-los e modificá-los, bem como para identificar dispositivos manual ou automaticamente.

Sobre as tags de dispositivo

O Kaspersky Security Center Cloud Console permite aplicar tags nos dispositivos. Uma *tag* é um rótulo de um dispositivo que pode ser usada para agrupar, descrever ou localizar dispositivos. As tags atribuídas aos dispositivos podem ser usadas para criar seleções, para localizar dispositivos e para distribuir dispositivos entre grupos de administração.

Você pode identificar os dispositivos manualmente ou automaticamente. Você pode usar a identificação manual quando quiser identificar um dispositivo individual. A autoidentificação é executada pelo Kaspersky Security Center Cloud Console de acordo com as regras de identificação especificadas.

Os dispositivos são identificados automaticamente quando as regras especificadas são atendidas. Uma regra individual corresponde a cada tag. As regras são aplicadas às propriedades da rede do dispositivo, sistema operacional, aplicativos instalados no dispositivo e outras propriedades de dispositivo. Por exemplo, se sua rede incluir dispositivos executando Windows, Linux e macOS, será possível configurar uma regra que atribuirá a tag `[Linux]` a todos os dispositivos baseados em Linux. Então, é possível usar essa tag ao criar uma seleção de dispositivos; isso ajudará a classificar todos os dispositivos baseados em Linux e atribuir-lhes uma tarefa. A tag é automaticamente removida de um dispositivo nos seguintes casos:

- Quando o dispositivo deixa de atender às condições da regra que atribui a tag.
- Quando a regra que atribui a tag é desativada ou excluída.

A lista de tags e a lista de regras em cada Servidor de Administração são independentes de todos outros Servidores de Administração, inclusive um Servidor de Administração principal ou Servidores de Administração virtuais subordinados. Uma regra é aplicada somente a dispositivos do mesmo Servidor de Administração no qual a regra é criada.

Criando uma tag de dispositivo

Para criar uma tag de dispositivo:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tags** → **Tags de dispositivos**.
2. Clique em **Adicionar**.
   Uma nova janela de tag é exibida.
3. No campo **Tag**, insira um nome de tag.
4. Clique em **Salvar** para salvar as alterações.

A nova tag aparece na lista de tags de dispositivo.

Renomeando uma tag de dispositivo

Para renomear uma tag de dispositivo:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tags** → **Tags de dispositivos**.
2. Clique no nome da tag que deseja renomear.
   A janela de propriedades do identificador é exibida.
3. No campo **Tag**, altere o nome da tag.
4. Clique em **Salvar** para salvar as alterações.

A tag atualizada aparece na lista de tags de dispositivo.

Excluindo uma tag de dispositivo

Para excluir uma tag de dispositivo:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tags** → **Tags de dispositivos**.
2. Na lista, selecione a tag de dispositivo que deseja excluir.
3. Clique no botão **Excluir**.
4. Na janela que se abre, clique em **Sim**.

A tag de dispositivo é excluída. A tag excluída é automaticamente removida de todos os dispositivos aos quais foi atribuída.

A tag excluída não é removida automaticamente das regras de codificação automática. Após a tag ser excluída, ela será atribuída a um novo dispositivo apenas quando o dispositivo atender primeiro às condições de uma regra que atribui a tag.

A tag excluída não é removida automaticamente do dispositivo caso ela seja atribuída ao dispositivo por um aplicativo ou Agente de Rede. Para remover a tag do seu dispositivo, use o utilitário klscflag.

Visualizando dispositivos aos quais uma tag está atribuída

Para visualizar dispositivos aos quais uma tag está atribuída:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tags** → **Tags de dispositivos**.
2. Clique no link **Visualizar dispositivos** ao lado da tag para a qual deseja visualizar os dispositivos atribuídos.

A lista de dispositivos exibida mostra apenas os dispositivos aos quais a tag está atribuída.

Para retornar à lista de tags de dispositivo, clique no botão **Voltar** do navegador.

Visualizando as tags atribuídas a um dispositivo

Para visualizar as tags atribuídas a um dispositivo:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo cujas tags deseja visualizar.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Tags**.

A lista de tags atribuídas ao dispositivo selecionado é exibida.

Você pode atribuir outra tag ao dispositivo ou remover uma tag já atribuída. Você também pode ver todas as tags de dispositivo existentes no Servidor de Administração.

Marcar dispositivos manualmente

Para atribuir uma tag a um dispositivo:

1. Visualize as tags atribuídas ao dispositivo ao qual deseja atribuir outra tag.
2. Clique em **Adicionar**.
3. Na janela que se abre, execute uma das seguintes ações:
   - Para criar e atribuir uma nova tag, selecione **Criar nova tag** e especifique o nome da nova tag.
   - Para selecionar uma tag existente, selecione **Atribuir tag existente** e depois selecione a tag desejada na lista suspensa.
4. Clique em **OK** para aplicar as alterações.
5. Clique em **Salvar** para salvar as alterações.

A tag selecionada é atribuída ao dispositivo.

Para atribuir uma tag a vários dispositivos:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.
2. Selecione os dispositivos aos quais você deseja atribuir uma tag.
3. Clique em **Tags** e selecione **Atribuir** na lista suspensa.
4. Na janela exibida, selecione uma tag na lista suspensa.
   Se necessário, você pode selecionar várias tags.
   Você também pode fazer o seguinte:
   - Edite o nome de uma tag clicando no ícone **Editar** (✎).
     Especifique o novo nome da tag e clique no botão **Salvar**.

     > Observe que a tag também será renomeada na lista de tags de dispositivo.

   - Exclua uma tag clicando no ícone **Excluir** (🗑).
     Na janela exibida, clique em **Excluir**.

     > Observe que a tag também será excluída do Servidor de Administração.

5. Clique no botão **Salvar**.

As tags são atribuídas ao dispositivos selecionados. Você pode remover as tags atribuídas.

Removendo tags atribuídas de dispositivos

A tag de dispositivo não atribuída não é excluída. Se quiser, você poderá excluí-lo manualmente.

Não é possível remover manualmente as tags atribuídas ao dispositivo por aplicativos ou pelo Agente de Rede. Para remover essas tags, use o utilitário klscflag.

Para remover uma tag de um dispositivo:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo cujas tags deseja visualizar.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Tags**.
4. Marque a caixa de seleção ao lado da tag que deseja remover.
5. No topo da lista, clique no botão **Desatribuir tag**.
6. Na janela que se abre, clique em **Sim**.

   A tag é removida do dispositivo.

Para remover tags de vários dispositivos:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.
2. Selecione os dispositivos cujas tags você deseja remover.
3. Clique em **Tags** e selecione **Remover** na lista suspensa.
4. Na janela exibida, marque as caixas de seleção ao lado das tags que deseja remover.

   A janela exibe todas as tags atribuídas a todos os dispositivos selecionados na etapa 2.

5. Clique no botão **Salvar**.

   As tags são removidas dos dispositivos.

Visualização de regras para identificar dispositivos automaticamente

Para visualizar regras para identificar dispositivos automaticamente,

Execute alguma das seguintes ações:

- No menu principal, vá para **Ativos (dispositivos)** → **Tags** → **Regras de aplicação automática de tags**.

- No menu principal, vá para **Ativos (dispositivos)** → **Tags** → **Tags de dispositivos** e, em seguida, clique no link **Configurar regras de aplicação automática de tags**.
- Visualize as tags atribuídas a um dispositivo e depois clique no botão **Configurações**.

A lista de regras para identificar dispositivos automaticamente é exibida.

Edição de uma regra para identificar dispositivos automaticamente

Para editar uma regra para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Clique no nome da regra que deseja editar.

   Uma janela de configurações de regra é exibida.
3. Edite as propriedades gerais da regra:

   a. No campo **Nome da regra**, altere o nome da regra.

   O nome não pode conter mais de 256 caracteres.

   b. Execute alguma das seguintes ações:

   - Ative a regra mudando o botão de alternar para **Regra ativada**.
   - Desative a regra mudando o botão de alternar para **Regra desativada**.
4. Execute alguma das seguintes ações:

   - Se desejar adicionar uma nova condição, clique no botão **Adicionar** e especifique as configurações da nova condição na janela aberta.
   - Se deseja editar uma condição existente, clique no nome da condição que quer editar e edite as configurações de condição.
   - Se deseja excluir uma condição, marque a caixa de seleção ao lado do nome da condição que deseja excluir e clique em **Excluir**.
5. Clique em **OK** na janela de configurações de condições.
6. Clique em **Salvar** para salvar as alterações.

A regra editada é mostrada na lista.

Criação de uma regra para identificar dispositivos automaticamente

Para criar uma regra para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Clique em **Adicionar**.

   Uma nova janela de configurações de regra é exibida.

3. Configure as propriedades gerais da regra:

   a. No campo **Nome da regra**, insira o novo nome da regra.

      O nome não pode conter mais de 256 caracteres.

   b. Execute uma das seguintes ações:

      - Ative a regra mudando o botão de alternar para **Regra ativada**.
      - Desative a regra mudando o botão de alternar para **Regra desativada**.

   c. No campo **Tag**, digite o novo nome da tag de dispositivo ou selecione uma das tags de dispositivo existentes na lista.

      O nome não pode conter mais de 256 caracteres.

4. Na seção de condições, clique no botão **Adicionar** para adicionar uma nova condição.

   Uma nova janela de configurações de condição é exibida.

5. Insira o nome da condição.

   O nome não pode conter mais de 256 caracteres. O nome deve ser exclusivo em uma regra.

6. Defina o acionamento da regra de acordo com as seguintes condições. Você pode selecionar múltiplas condições.

   - **Rede** – Propriedades da rede do dispositivo, tal como o nome do dispositivo na rede Windows, ou a inclusão do dispositivo em um domínio ou em uma subrede IP.

     Caso o agrupamento com distinção entre maiúsculas e minúsculas seja definido para o banco de dados usado para o Kaspersky Security Center Cloud Console, mantenha maiúsculas e minúsculas ao especificar um nome DNS de dispositivo. Caso contrário, a regra de marcação automática não funcionará.

   - **Aplicativos** – Presença do Agente de Rede no dispositivo, tipo de sistema operacional, versão e arquitetura.
   - **Máquinas virtuais** – O dispositivo pertence a um tipo específico da máquina virtual.
   - **Active Directory** – Presença do dispositivo em uma unidade organizacional do Active Directory e a associação do dispositivo em um grupo do Active Directory.
   - **Registro de aplicativos** – Presença de aplicativos de diferentes fornecedores no dispositivo.

7. Clique em **OK** para salvar as alterações.

   Se necessário, você pode definir múltiplas condições para única regra. Neste caso, a tag será atribuída um dispositivo se atender ao menos uma condição.

8. Clique em **Salvar** para salvar as alterações.

A regra recém-criada entra em vigor nos dispositivos gerenciados pelo Servidor de Administração selecionado. Se as configurações de um dispositivo atenderem as condições da regra, ao dispositivo é atribuído à tag.

Depois, a regra é aplicada nos seguintes casos:

- Automática e periodicamente, dependendo da carga de trabalho de servidor

- Depois que você editar a regra
- Quando você executar a regra manualmente
- Depois que o Servidor de Administração detectar uma modificação nas configurações de um dispositivo que atende às condições de regra ou nas configurações de um grupo que contém tal dispositivo

Você pode criar múltiplas regras de identificação. A um dispositivo único pode ser atribuído múltiplas regras de identificação e se as respetivas condições destas regras forem atendidas simultaneamente. Você pode exibir a lista de todas as tags atribuídas nas propriedades do dispositivo.

Execução de regras para identificar dispositivos automaticamente

Quando uma regra é executada, a tag especificada nas propriedades dessa regra é atribuída aos dispositivos que atendem às condições especificadas nas propriedades da mesma regra. Você pode executar apenas regras ativas.

Para executar regras para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Marque as caixas de seleção ao lado das regras ativas que você deseja executar.
3. Clique no botão **Executar regra**.

   As regras selecionadas são executadas.

Exclusão de uma regra para identificar dispositivos automaticamente

Para excluir uma regra para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Marque a caixa de seleção ao lado da regra que você deseja excluir.
3. Clique em **Excluir**.
4. Na janela exibida, clique em **Excluir** novamente.

   A regra selecionada é excluída. A tag especificada nas propriedades dessa regra tem a atribuição removida de todos dos dispositivos aos quais foi atribuída.

> A tag de dispositivo não atribuída não é excluída. Se quiser, você poderá excluí-lo manualmente.

Quarentena e Backup

Os aplicativos de antivírus da Kaspersky instalados em dispositivos cliente podem colocar arquivos em Quarentena ou Backup durante a verificação do dispositivo.

Quarentena é um repositório especial que armazena prováveis arquivos infectados com vírus e arquivos que não podem ser desinfectados no momento que são encontrados.

O *Backup* é designado para armazenar cópias backup dos arquivos que foram excluídos ou modificados durante o processo de desinfecção.

O Kaspersky Security Center Cloud Console cria uma lista resumida dos arquivos colocados em Quarentena ou Backup pelos aplicativos da Kaspersky nos dispositivos cliente. Os Agentes de Rede em dispositivos cliente transferem as informações sobre os arquivos em Quarentena e Backup para o Servidor de Administração.

O Kaspersky Security Center Cloud Console não copia arquivos de repositórios para o Servidor de Administração. Todos os arquivos são armazenados nos repositórios nos dispositivos.

Download de um arquivo dos repositórios

O Kaspersky Security Center Cloud Console permite baixar cópias de arquivos colocadas em quarentena ou criadas em backup por um aplicativo de segurança em um dispositivo cliente. Os arquivos são copiados no destino especificado.

É possível baixar os arquivos se apenas uma das duas condições a seguir for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo, um servidor push estiver em uso ou um gateway de conexão estiver em uso. Caso contrário, não será possível fazer o download.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Para salvar uma cópia do arquivo da Quarentena ou Backup para o disco rígido:

1. Execute uma das seguintes ações:

   - Caso queira salvar uma cópia do arquivo da Quarentena, No menu principal, vá para **Operações** → **Repositórios** → **Quarentena**.

   - Caso queira salvar uma cópia do arquivo a partir do Backup, No menu principal, vá para **Operações** → **Repositórios** → **Backup**.

2. Na janela que se abre, selecione um arquivo que deseja baixar e clique em **Baixar**.

   O download é iniciado. Uma cópia do arquivo que foi colocado em Quarentena no dispositivo cliente é salva na pasta especificada.

Excluir os arquivos dos repositórios

Para excluir um arquivo de Quarentena ou Backup:

1. Execute uma das seguintes ações:

   - Caso queira salvar uma cópia do arquivo da Quarentena, No menu principal, vá para **Operações** → **Repositórios** → **Quarentena**.

- Caso queira salvar uma cópia do arquivo a partir do Backup, No menu principal, vá para **Operações** → **Repositórios** → **Backup**.

2. Na janela que se abre, selecione um arquivo que deseja excluir e clique em **Excluir**.

3. Confirme que deseja excluir o arquivo.

O aplicativo de segurança no dispositivo cliente que colocou os arquivos no repositório (Quarentena ou Backup) exclui os mesmos arquivos desse repositório.

Diagnóstico remoto de dispositivos cliente

É possível usar o diagnóstico remoto para execução remota das seguintes operações nos dispositivos clientes baseados em Windows e Linux:

- Ativar e desativar o rastreamento, alterar o nível de rastreamento e baixar o arquivo de rastreamento
- Download de informações do sistema e de configurações do aplicativo
- Download de registros de eventos
- Gerar um arquivo de dump para um aplicativo
- Início do diagnóstico e download de seus relatórios
- Início, interrupção e reinício de aplicativos

Você pode usar registros de eventos e relatórios de diagnóstico baixados de um dispositivo cliente para resolver problemas. Além disso, ao entrar em contato com o Suporte Técnico da Kaspersky, um especialista de Suporte Técnico pode pedir que você faça download de arquivos de rastreamento, arquivos de despejo, logs de eventos e relatórios de diagnóstico de um dispositivo cliente para análise adicional na Kaspersky.

Abertura da janela de diagnóstico remoto

Para executar diagnóstico remoto em dispositivos clientes baseados em Windows e Linux, é necessário abrir a janela de diagnóstico remoto.

Para abrir a janela de diagnóstico remoto:

1. Para selecionar o dispositivo para o qual você deseja abrir a janela de diagnóstico remoto, execute um dos seguintes procedimentos:

   - Se o dispositivo pertencer a um grupo de administração, vá para **Ativos (dispositivos)** → **Grupos** → **<nome do grupo>** → **Dispositivos gerenciados**.

   - Caso o dispositivo pertença ao grupo de dispositivos não atribuídos, No menu principal, vá para **Descoberta e implementação** → **Dispositivos não atribuídos**.

2. Clique no nome do dispositivo necessário.

3. Na janela de propriedades do dispositivo exibida, selecione a guia **Avançado**.

4. Na janela que é aberta, clique em **Diagnóstico remoto**.

   Isso abre a janela de **Diagnóstico remoto** do dispositivo cliente. Caso a conexão entre o Servidor de Administração e o dispositivo cliente não seja estabelecida, uma mensagem de erro é exibida.

Como alternativa, caso precise obter todas as informações de diagnóstico sobre um dispositivo cliente baseado em Linux de uma só vez, é possível executar o script collect.sh nesse dispositivo.

Ativação e desativação do rastreamento para aplicativos

É possível ativar e desativar o rastreamento para aplicativos, incluindo o rastreamento do Xperf.

Ativação e desativação do rastreamento

Para ativar ou desativar o rastreamento em um dispositivo remoto:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione o aplicativo para o qual deseja ativar ou desativar o rastreamento.

   A lista de opções de diagnóstico remoto é aberta.
4. Se desejar ativar o rastreamento:

   a. Na seção **Rastreamento**, clique em **Ativar rastreamento**.

   b. Na janela **Modificar nível de rastreamento** que se abre, recomendamos que você mantenha os valores padrões das configurações. Quando necessário, um especialista de Suporte Técnico orientará você através do processo de configuração. Estão disponíveis as seguintes configurações:

   - **Nível de rastreamento**

     O nível de rastreamento define o volume de detalhes que o arquivo de rastreamento contém.

   - **Rastreamento baseado em rotatividade**

     O aplicativo sobrescreve as informações de rastreamento para impedir o aumento excessivo no tamanho do arquivo de rastreamento. Especifique o número máximo de arquivos a serem usados para armazenar as informações de rastreamento e o tamanho máximo de cada arquivo. Se o número máximo de arquivos de rastreamento com o tamanho máximo estiver gravado, o arquivo de rastreamento mais antigo será excluído para que um novo arquivo possa ser gravado.

     Essa configuração está disponível apenas para o Kaspersky Endpoint Security.

   c. Clique em **Salvar**.

   O rastreamento está ativado para o aplicativo selecionado. Em alguns casos, um aplicativo de segurança e sua tarefa devem ser reiniciados para que seja possível ativar o rastreamento.

Em dispositivos clientes baseados em Linux, o rastreamento do componente Atualizador do Kaspersky Security Agent é regulado pelas configurações do Agente de Rede. Portanto, as opções **Ativar rastreamento** e **Modificar nível de rastreamento** estão desativadas para este componente em dispositivos clientes que executam o Linux.

5. Caso deseje desativar o rastreamento para o aplicativo selecionado, clique em **Desabilitar rastreamento**.

   O rastreamento está desativado para o aplicativo selecionado.

Ativação do rastreamento do Xperf

Para o Kaspersky Endpoint Security, um especialista de Suporte Técnico pode solicitar que você ative o rastreamento do Xperf para obter informações sobre o desempenho do sistema.

Para ativar e configurar o rastreamento do Xperf ou desativá-lo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.

2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.

3. Na lista de aplicativos, selecione Kaspersky Endpoint Security for Windows.

   A lista de opções de diagnóstico remoto do Kaspersky Endpoint Security for Windows é exibida.

4. Na seção **Rastreamento do Xpref** da lista, clique em **Ativar rastreamento Xperf**.

   Se o rastreamento do Xperf já estiver ativado, o botão **Desativar rastreamento Xperf** é exibido. Clique neste botão caso queira desativar o rastreamento do Xperf para o Kaspersky Endpoint Security for Windows.

5. Na janela **Alterar nível de rastreamento Xperf** que se abre, dependendo da solicitação do especialista de Suporte Técnico, faça o seguinte:

   a. Selecione um dos seguintes níveis de rastreamento:

   - **Nível leve**

     Um arquivo de rastreamento deste tipo contém a quantidade mínima de informações sobre o sistema.

     Por padrão, esta opção está selecionada.

   - **Nível profundo**

     Um arquivo de rastreamento deste tipo contém informações mais detalhadas do que as dos arquivos de rastreamento do tipo *Superficial* e podem ser solicitadas pelos especialistas de Suporte Técnico quando um arquivo de rastreamento do tipo *Superficial* não for suficiente para a avaliação de desempenho. Um arquivo de rastreamento *Profundo* contém informações técnicas sobre o sistema, como as informações sobre hardware, sistema operacional, lista de processos e aplicativos iniciados e concluídos, eventos usados para avaliação de desempenho e eventos da Ferramenta de Avaliação de Sistema do Windows.

   b. Selecione um dos seguintes tipos de rastreamento do Xperf:

- **Tipo básico**

  As informações de rastreamento são recebidas durante a operação do aplicativo Kaspersky Endpoint Security.

  Por padrão, esta opção está selecionada.

- **Tipo na reinicialização**

  As informações de rastreamento são recebidas quando o sistema operacional é iniciado no dispositivo gerenciado. Esse tipo de rastreamento é eficaz quando o problema que afeta o desempenho do sistema ocorre depois que o dispositivo é ligado e antes da inicialização do Kaspersky Endpoint Security.

Você também pode receber a solicitação de ativar a opção **Tamanho do arquivo de rotatividade, em MB** para impedir o aumento excessivo no tamanho do arquivo de rastreamento. Especifique o tamanho máximo do arquivo de rastreamento. Quando o arquivo atingir o tamanho máximo, as informações de rastreamento mais antigas serão substituídas por novas informações.

c. Defina o tamanho do arquivo de rotação.

d. Clique em **Salvar**.

O rastreamento do Xperf está ativado e configurado.

6. Caso queira desativar o rastreamento do Xperf para o Kaspersky Endpoint Security for Windows, clique em **Desativar rastreamento Xperf** na seção **Rastreamento do Xpref**.

   O rastreamento do Xperf está desativado.

Download de arquivos de rastreamento de um aplicativo

É possível baixar os arquivos de rastreamento a partir de um dispositivo cliente se apenas uma das duas condições a seguir for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo, um servidor push estive em uso ou um gateway de conexão estiver em uso. Caso contrário, não será possível fazer o download.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Para fazer download do arquivo de rastreamento de um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.

2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.

3. Na lista de aplicativos, selecione o aplicativo para o qual deseja baixar o arquivo de rastreamento.

4. Na seção **Rastreamento**, clique no botão **Arquivos de rastreamento**.

   Assim, a janela **Registros de rastreamento do dispositivo** é aberta, onde uma lista de arquivos de rastreamento é exibida.

5. Na lista de arquivos de rastreamento, selecione o arquivo que deseja baixar.

6. Execute uma das seguintes ações:

   - Faça o download do arquivo selecionado clicando em **Baixar**. É possível selecionar um ou vários arquivos para baixar.

   - Baixe uma parte do arquivo selecionado:

     a. Clique em **Baixar uma parte**.

     Não é possível baixar partes de vários arquivos ao mesmo tempo. Caso selecione mais de um arquivo de rastreamento, o botão **Baixar uma parte** será desativado.

     b. Na janela exibida, especifique o nome e a parte do arquivo a ser baixada, de acordo com suas necessidades.

     Para dispositivos baseados em Linux, a edição do nome da parte do arquivo não está disponível.

     c. Clique em **Baixar**.

O arquivo selecionado, ou sua parte, é baixado no local especificado.

Exclusão de arquivos de rastreamento

É possível excluir arquivos de rastreamento que não sejam mais necessários.

Para excluir um arquivo de rastreamento:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.

2. Na janela de diagnóstico remoto que é aberta, selecione a guia **Registros de evento**.

3. Na seção **Arquivos de rastreamento**, clique em **Logs do Windows Update** ou **Logs de instalação remota**, dependendo de quais arquivos de rastreamento deseja excluir.

   Assim, a janela **Registros de rastreamento do dispositivo** é aberta, onde uma lista de arquivos de rastreamento é exibida.

4. Na lista de arquivos de rastreamento, selecione um ou vários arquivos que deseja excluir.

5. Clique no botão **Remover**.

Os arquivos de rastreamento selecionados são excluídos.

Download das configurações do aplicativo

É possível baixar as configurações do aplicativo de um dispositivo cliente se apenas uma das condições a seguir for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo, um servidor push estiver em uso ou se um gateway de conexão estiver em uso. Caso contrário, não será possível fazer o download.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Para baixar as configurações do aplicativo a partir de um dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.
3. Na seção **Configurações do aplicativo**, clique no botão **Baixar** para baixar as informações sobre as configurações dos aplicativos instalados no dispositivo cliente.

O arquivo ZIP com as informações é baixado no local especificado.

Download das informações do sistema de um dispositivo cliente

É possível baixar as informações do sistema para o dispositivo a partir de um dispositivo cliente se apenas uma das seguintes condições for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo, um servidor push estiver em uso ou um gateway de conexão estiver em uso. Caso contrário, não será possível fazer o download.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Para baixar as informações do sistema a partir de um dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Informações do sistema**.
3. Clique no botão **Baixar** para baixar as informações do sistema sobre o dispositivo cliente.

O arquivo com as informações é baixado para o local especificado.

Download de registros de eventos

É possível baixar os logs de eventos para o seu dispositivo a partir de um dispositivo cliente se apenas uma das seguintes condições for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo, um servidor push estiver em uso ou um gateway de conexão estiver em uso. Caso contrário, não será possível fazer o download.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Para baixar um log de eventos a partir de um dispositivo remoto:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, na guia **Registros de evento**, clique em **Todos os logs do dispositivo**.
3. Na janela **Todos os logs do dispositivo**, selecione os logs relevantes.
4. Execute uma das seguintes ações:
   - Baixe o log selecionado clicando em **Baixar todo o arquivo**.

- Baixe uma parte do log selecionado:

  a. Clique em **Baixar uma parte**.

  Não é possível baixar partes de vários logs ao mesmo tempo. Caso mais de uma política seja selecionada, o botão **Baixar uma parte** será desabilitado.

  b. Na janela exibida, especifique o nome e a parte do arquivo a ser baixada de acordo com suas necessidades.

  c. Clique em **Baixar**.

O log de eventos selecionado, ou uma parte dele, é baixado no local especificado.

Início, interrupção e reinício do aplicativo

É possível iniciar, parar e reiniciar aplicativos em um dispositivo cliente.

Para iniciar, interromper ou reiniciar um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione o aplicativo que deseja iniciar, parar ou reiniciar.
4. Selecione uma ação clicando em um dos seguintes botões:

   - **Parar aplicativo**

     Esse botão está disponível apenas se o aplicativo estiver em execução no momento.
   - **Reiniciar aplicativo**

     Esse botão está disponível apenas se o aplicativo estiver em execução no momento.
   - **Iniciar aplicativo**

     Esse botão está disponível apenas se o aplicativo não estiver em execução no momento.

Dependendo da ação selecionada, o aplicativo necessário é iniciado, parado ou reiniciado no dispositivo cliente.

Se o Agente de Rede for reiniciado, será exibida uma mensagem informando que a conexão atual do dispositivo com o Servidor de Administração será perdida.

Execução do diagnóstico remoto de um aplicativo e download dos resultados

Para iniciar o diagnóstico para um aplicativo em um dispositivo remoto e baixar os resultados:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.

Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.

3. Na lista de aplicativos, selecione o aplicativo para o qual deseja executar o diagnóstico remoto.

   A lista de opções de diagnóstico remoto é aberta.

4. Na seção **Relatório de diagnóstico**, clique no botão **Executar diagnósticos**.

   Isso inicia o processo de diagnóstico remoto e gera um relatório de diagnóstico. Quando o processo de diagnóstico estiver concluído, o botão **Baixar o relatório de diagnóstico** ficará disponível.

5. Clique no botão **Baixar o relatório de diagnóstico** para baixar o relatório.

O relatório é baixado no local especificado.

Execução de um aplicativo em um dispositivo cliente

Você pode ter que executar um aplicativo no dispositivo cliente se um especialista de suporte da Kaspersky solicitar. Não será necessário instalar o aplicativo no dispositivo. Não será necessário instalar o aplicativo no dispositivo.

Para executar um aplicativo no dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.

2. Na janela de diagnóstico remoto, selecione a guia **Executando um aplicativo remoto**.

3. Na seção **Arquivos do aplicativo**, clique no botão **Procurar** para selecionar um arquivo ZIP contendo o aplicativo que deseja executar no dispositivo cliente.

   > O arquivo comprimido deve incluir a pasta do utilitário. Essa pasta contém o arquivo executável a ser executado em um dispositivo remoto.

   É possível especificar o nome do arquivo executável e os argumentos da linha de comando, caso seja necessário. Para fazer isso, preencha os campos **Arquivo executável em um arquivo comprimido para ser executado em um dispositivo remoto** e os campos **Argumentos da linha de comando**.

4. Clique no botão **Carregar e executar** para executar o aplicativo especificado em um dispositivo cliente.

5. Siga as instruções do especialista de suporte da Kaspersky.

Gerar um arquivo de dump para um aplicativo

Um arquivo de despejo do aplicativo permite visualizar os parâmetros do aplicativo em execução em um dispositivo cliente em um dado momento. Esse arquivo também contém informações sobre os módulos que foram carregados para um aplicativo.

> A geração de arquivos de despejo está disponível apenas para processos de 32 bits em execução em dispositivos cliente baseados no Windows. Para dispositivos cliente que executam Linux e para processos de 64 bits, esse recurso não é compatível.

Para criar um arquivo de despejo para um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, clique na guia **Executando um aplicativo remoto**.
3. Na seção **Gerando o arquivo de dump do processo**, especifique o arquivo executável do aplicativo para o qual deseja gerar um arquivo de despejo.
4. Clique no botão **Baixar** para salvar o arquivo de despejo do aplicativo especificado.

   Caso o aplicativo especificado não esteja em execução no dispositivo cliente, a mensagem de erro será exibida.

Conexão remota à Área de trabalho de um dispositivo cliente

É possível obter acesso remoto à área de trabalho de um dispositivo cliente através de um Agente de Rede instalado no dispositivo. A conexão remota a um dispositivo por meio do Agente de Rede é possível mesmo que as portas TCP e UDP do dispositivo cliente estejam fechadas.

Ao estabelecer a conexão com o dispositivo, o acesso completo às informações armazenadas nele é obtido para gerenciar os aplicativos instalados.

A conexão remota deve ser permitida nas configurações do sistema operacional do dispositivo gerenciado de destino. Por exemplo, no Windows 10, essa opção é chamada **Permitir conexões de Assistência Remota para este computador** (é possível encontrar essa opção em **Painel de controle** → **Sistema e Segurança** → **Sistema** → **Configurações remotas**). Caso tenha uma licença para o recurso de Gerenciamento de patches e vulnerabilidades, será possível ativar a opção à força ao estabelecer a conexão com um dispositivo gerenciado. Caso não tenha a licença, ative essa opção localmente no dispositivo gerenciado de destino. Se esta opção estiver desativada, a conexão remota não é possível.

Para estabelecer uma conexão remota com um dispositivo, você deve ter dois utilitários:

- Utilitário Kaspersky chamado klsctunnel. O utilitário deve ser armazenado na estação de trabalho. Este utilitário é usado para encapsular a conexão entre um dispositivo cliente e o Servidor de Administração.

  O Kaspersky Security Center Cloud Console permite o tunelamento de conexões TCP a partir do Console de Administração por meio do Servidor de Administração, e, depois, por meio do Agente de Rede, a uma porta especificada em um dispositivo gerenciado. O tunelamento é projetado para conectar um aplicativo cliente em um dispositivo com o Console de Administração instalado à uma porta TCP em um dispositivo gerenciado – se nenhuma conexão direta for possível entre o Console de Administração e o dispositivo alvo.

  A conexão em túnel entre um dispositivo cliente remoto e Servidor de Administração é necessária se a porta usada para a conexão ao Servidor de Administração não estiver disponível no dispositivo. A porta no dispositivo poderá estar indisponível nos seguintes casos:

  - O dispositivo remoto é conectado à uma rede local que usa o mecanismo NAT.
  - Um dispositivo remoto é parte da rede local, do Servidor de Administração, mas sua porta está fechada por um firewall.

- Componente padrão do Microsoft Windows denominado Conexão de Área de Trabalho Remota. A conexão com uma área de trabalho remota é estabelecida através do utilitário Windows padrão mstsc.exe, de acordo com as configurações do utilitário.

A conexão com a sessão de área de trabalho remota atual do usuário é estabelecida sem o conhecimento do usuário. Uma vez conectado à sessão, o dispositivo do usuário será desconectado da sessão sem uma notificação prévia.

Para conectar-se com a área de trabalho de um dispositivo cliente, uma das seguintes condições deve ser satisfeita:

- O dispositivo cliente é membro de um grupo de administração que possui um ponto de distribuição com a opção **Não desconectar do Servidor de Administração** ativada.
- Nas configurações do dispositivo cliente, a opção **Não desconectar do Servidor de Administração** está ativada.

  O número total máximo de dispositivos clientes com a opção **Não desconectar do Servidor de Administração** ativada é de 300.

Para se conectar à Área de trabalho de um dispositivo cliente:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados.**
2. Marque a caixa de seleção ao lado do nome do dispositivo ao qual deseja obter acesso.
3. Clique no botão **Conectar-se à área de trabalho remota**.

   A janela Desktop remoto (somente Windows) se abre.
4. Clique no botão **Baixar** para baixar o utilitário klsctunnel.
5. Clique no botão **Copiar para transferência** para copiar o texto do campo de texto. Este texto é um objeto de dados binário (BLOB) que contém as configurações necessárias para estabelecer a conexão entre o Servidor de Administração e o dispositivo gerenciado.

   Um BLOB é válido por 3 minutos. Se ele expirou, reabra a janela Desktop remoto (somente Windows) para gerar um novo BLOB.
6. Execute o utilitário klsctunnel.

   A janela do utilitário é exibida.
7. Cole o texto copiado no campo de texto.
8. Se você usa um servidor proxy, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão do servidor proxy.
9. Clique no botão **Abrir porta**.

   A janela de login da Conexão de Área de Trabalho Remota é aberta.
10. Especifique as credenciais da conta na qual está atualmente conectado ao Kaspersky Security Center Cloud Console.
11. Clique no botão **Conectar**.

Quando a conexão com o dispositivo for estabelecida, a área de trabalho ficará disponível na janela Conexão remota do Microsoft Windows.

Conexão com dispositivos cliente através do Windows Desktop Sharing

É possível obter acesso remoto à área de trabalho de um dispositivo cliente através de um Agente de Rede instalado no dispositivo. A conexão remota a um dispositivo por meio do Agente de Rede é possível mesmo que as portas TCP e UDP do dispositivo cliente estejam fechadas.

É possível conectar-se a uma sessão existente em um dispositivo cliente sem desconectar o usuário desta sessão. Nesse caso, você e o usuário da sessão no dispositivo compartilham o acesso à área de trabalho.

Para estabelecer uma conexão remota com um dispositivo, você deve ter dois utilitários:

- Utilitário Kaspersky chamado klsctunnel. O utilitário deve ser armazenado na estação de trabalho. Este utilitário é usado para encapsular a conexão entre um dispositivo cliente e o Servidor de Administração.

  O Kaspersky Security Center Cloud Console permite o tunelamento de conexões TCP a partir do Console de Administração por meio do Servidor de Administração, e, depois, por meio do Agente de Rede, a uma porta especificada em um dispositivo gerenciado. O tunelamento é projetado para conectar um aplicativo cliente em um dispositivo com o Console de Administração instalado à uma porta TCP em um dispositivo gerenciado – se nenhuma conexão direta for possível entre o Console de Administração e o dispositivo alvo.

  A conexão em túnel entre um dispositivo cliente remoto e Servidor de Administração é necessária se a porta usada para a conexão ao Servidor de Administração não estiver disponível no dispositivo. A porta no dispositivo poderá estar indisponível nos seguintes casos:

  - O dispositivo remoto é conectado à uma rede local que usa o mecanismo NAT.
  - Um dispositivo remoto é parte da rede local, do Servidor de Administração, mas sua porta está fechada por um firewall.

- Compartilhamento da área de trabalho do Windows. Ao conectar-se a uma sessão existente da área de trabalho remota, o usuário da sessão no dispositivo recebe uma solicitação de conexão sua. Nenhuma informação sobre a atividade remota no dispositivo nem seus resultados serão salvos em relatórios criados pelo Kaspersky Security Center Cloud Console.

  É possível configurar uma auditoria da atividade do usuário em um dispositivo cliente remoto. Durante a auditoria, o aplicativo salva as informações sobre os arquivos que tenham sido abertos e/ou modificados pelo administrador no dispositivo cliente.

Para conectar-se com a área de trabalho de um dispositivo cliente por meio do Compartilhamento da área de trabalho do Windows, as seguintes condições devem ser satisfeitas:

- O Microsoft Windows Vista ou posterior está instalado em sua estação de trabalho.

  Para verificar se o recurso de Compartilhamento da área de trabalho do Windows está incluído na sua edição do Windows, verifique se o CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} está incluído no registro de 32 bits.

- O Microsoft Windows Vista ou mais recente está instalado no dispositivo cliente.

- O Kaspersky Security Center Cloud Console usa uma licença para Gerenciamento de patches e vulnerabilidades.

- O dispositivo cliente é membro de um grupo de administração que possui um ponto de distribuição com a opção **Não desconectar do Servidor de Administração** ativada ou se esta opção estiver ativada nas configurações do dispositivo cliente.

  Observe que o número total máximo de dispositivos clientes com a opção **Não desconectar do Servidor de Administração** ativada é de 300.

Para conectar-se com a área de trabalho de um de dispositivo cliente através da tecnologia de Compartilhamento da área de trabalho do Windows:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.
2. Marque a caixa de seleção ao lado do nome do dispositivo ao qual deseja obter acesso.
3. Clique no botão **Windows Desktop Sharing**.

   O Assistente de Windows Desktop Sharing é aberto.
4. Clique no botão **Baixar** para baixar o utilitário klsctunnel e aguarde a conclusão do processo de download.

   Se você já tiver o utilitário klsctunnel, ignore esta etapa.
5. Clique no botão **Avançar**.
6. Selecione a sessão no dispositivo ao qual deseja se conectar e clique no botão **Avançar**.
7. No dispositivo de destino, na caixa de diálogo exibida, o usuário deve permitir uma sessão de compartilhamento de área de trabalho. Caso contrário, a sessão não será possível.

   Depois que o usuário do dispositivo confirma a sessão de compartilhamento da área de trabalho, a próxima página do assistente é aberta.
8. Clique no botão **Copiar para transferência** para copiar o texto do campo de texto. Este texto é um objeto de dados binário (BLOB) que contém as configurações necessárias para estabelecer a conexão entre o Servidor de Administração e o dispositivo gerenciado.

   > Um BLOB é válido por 3 minutos. Se ele tiver expirado, gere um novo BLOB.
9. Execute o utilitário klsctunnel.

   A janela do utilitário é exibida.
10. Cole o texto copiado no campo de texto.
11. Se você usa um servidor proxy, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão do servidor proxy.
12. Clique no botão **Abrir porta**.

O compartilhamento da área de trabalho é iniciado em uma nova janela. Caso queira interagir com o dispositivo, clique no ícone Menu () no canto superior esquerdo da janela e selecione **Modo interativo**.

Acionamento de regras no modo de Treinamento inteligente

Esta seção fornece informações sobre as detecções realizadas pelas regras do Controle Adaptativo de Anomalias no Kaspersky Endpoint Security for Windows em dispositivos cliente.

As regras detectam e podem bloquear comportamento anômalo nos dispositivos cliente. Se as regras funcionarem no modo de Treinamento Inteligente, elas detectarão o comportamento anômalo e enviarão relatórios sobre cada ocorrência ao Servidor de Administração do Kaspersky Security Center Cloud Console. Esta informação é armazenada como uma lista na subpasta **Acionamento de regras no estado de Treinamento inteligente** da pasta **Repositórios**. Você pode confirmar que as detecções estão corretas ou adicioná-las como exclusões para que esse tipo do comportamento não seja mais considerado como anômalo.

As informações sobre detecções são armazenadas no log de eventos no Servidor de Administração (junto com outros eventos) e no relatório do Controle Adaptativo de Anomalias.

Para mais informações sobre o controle adaptativo de anomalias, as regras, seus modos e status, consulte a ajuda do Kaspersky Endpoint Security.

Exibir a lista de detecções executadas usando regras do Controle Adaptativo de Anomalias

Para exibir a lista de detecções executadas usando regras do Controle Adaptativo de Anomalias:

1. No menu principal, acesse **Operações → Repositórios**.
2. Clique no link **Acionamento de regras no estado de Treinamento inteligente**.

   A lista exibe as seguintes informações sobre as detecções executadas usando regras do Controle Adaptativo de Anomalias:

   - **Grupo de administração**

     O nome do grupo de administração ao qual o dispositivo pertence.

   - **Nome do dispositivo**

     O nome do dispositivo cliente onde a regra foi aplicada.

   - **Nome**

     O nome da regra aplicada.

   - **Status**

     Excluir – Se o Administrador processou e adicionou este item como uma exclusão às regras. Este status permanecerá até a próxima sincronização do dispositivo cliente com o Servidor de Administração; após a sincronização, o item desaparecerá da lista.

     Confirmar – Se o Administrador processou e confirmou este item. Este status permanecerá até a próxima sincronização do dispositivo cliente com o Servidor de Administração; após a sincronização, o item desaparecerá da lista.

     Vazio – Se o Administrador não processou este item.

   - **Nome do usuário**

O nome do usuário de dispositivo cliente que executou o processo que gerou a detecção.

- **Processado**

  Data em que a anomalia foi detectada.

- **Caminho do processo de origem**

  Caminho até o processo de origem, isto é, até o processo que executa a ação (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do processo de origem**

  Hash SHA-256 do arquivo do processo de origem (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Caminho do objeto de origem**

  Caminho até o objeto que iniciou o processo (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do objeto de origem**

  Hash SHA-256 do arquivo de origem (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Caminho do processo de destino**

  Caminho até o processo de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do processo de destino**

  Hash SHA-256 do processo de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Caminho do objeto de destino**

  Caminho até o objeto de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do objeto de destino**

  Hash SHA-256 do processo de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

Para exibir propriedades de cada elemento de informação:

1. No menu principal, acesse **Operações → Repositórios**.
2. Clique no link **Acionamento de regras no estado de Treinamento inteligente**.
3. Na janela que se abre, selecione o objeto desejado.
4. Clique no link **Propriedades**.

   A janela de propriedades do objeto é aberta, exibindo informações sobre o elemento selecionado.

Você pode confirmar ou adicionar às exclusões qualquer elemento na lista de detecções das regras do Controle Adaptativo de Anomalias.

Para confirmar um elemento,

Selecione um elemento (ou vários) na lista de detecções e clique no botão **Confirmar**.

O status do(s) elemento(s) será alterado para **Confirmando**.

Sua confirmação contribuirá com as estatísticas usadas pelas regras (para obter mais informações, consulte a documentação do Kaspersky Endpoint Security for Windows).

Para adicionar um elemento como uma exclusão,

Selecione um elemento (ou vários) na lista de detecções e clique no botão **Excluir**.

O assistente para Adicionar exclusão é iniciado. Siga as instruções do Assistente.

Se você rejeitar ou confirmar um elemento, ele será excluído da lista de detecções após a próxima sincronização do dispositivo cliente com o Servidor de Administração e não será mais exibido na lista.

Adicionar exclusões a partir das regras do Controle Adaptativo de Anomalias

O assistente para Adicionar exclusão permite adicionar exclusões das regras de Controle Adaptativo de Anomalias para o Kaspersky Endpoint Security for Windows.

Para iniciar o assistente para Adicionar exclusão através do Controle Adaptativo de Anomalias:

1. No meu principal, acesse **Operações → Repositórios → Acionamento de regras no estado de Treinamento inteligente**.
2. Na janela aberta, selecione um elemento (ou vários) na lista de detecções e, em seguida, clique no botão **Excluir**.

   Você pode adicionar até 1.000 exclusões por vez. Se você selecionar mais elementos e tentar adicioná-los às exclusões, uma mensagem de erro será exibida.

O assistente para Adicionar exclusão é iniciado.

Políticas e perfis da política

No Kaspersky Security Center Cloud Console, você pode criar políticas para aplicativos da Kaspersky. Esta seção descreve políticas e perfis da política e fornece instruções para criá-las e modificá-las.

Sobre as políticas

Uma *política* é um conjunto de configurações do aplicativo Kaspersky, aplicadas a um grupo de administração e seus subgrupos. Você pode instalar vários aplicativos Kaspersky nos dispositivos de um grupo de administração. O Kaspersky Security Center Cloud Console fornece uma única política para cada aplicativo Kaspersky em um grupo de administração. Uma política tem um dos seguintes status (consulte a tabela abaixo):

O status da política

Status	Descrição
Ativo	A política atual aplicada ao dispositivo. Apenas uma política pode estar ativa por aplicativo Kaspersky em cada grupo de administração. Os dispositivos aplicam os valores de configuração de uma política ativa para um aplicativo Kaspersky.
Inativo	Uma política que não é aplicada atualmente a um dispositivo.
Ausência	Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

As políticas funcionam de acordo com as seguintes regras:

- Várias políticas com valores diferentes podem ser configuradas para um único aplicativo.
- Apenas uma política pode estar ativa para o aplicativo atual.
- É possível ativar uma política desativada quando um evento específico ocorre. Por exemplo, você pode forçar configurações de proteção antivírus mais rigorosas durante surtos de vírus.
- Uma política pode ter políticas secundárias.

Geralmente, você pode usar políticas como preparação para situações de emergência, como um ataque de vírus. Se houver um ataque por meio de unidades flash, você pode ativar uma política que bloqueie o acesso a unidades flash. Nesse caso, a política ativa atual torna-se automaticamente inativa.

Para evitar ter que efetuar manutenção de várias políticas, por exemplo, quando ocasiões diferentes pressupõem a alteração de várias configurações apenas, você pode usar perfis de política.

Um *perfil de política* é um subconjunto nomeado de valores de configuração que substitui os valores de configuração de uma política. Um perfil de política afeta a formação de configurações efetivas em um dispositivo gerenciado. *Configurações em vigor* são um conjunto de configurações de política, configurações de perfil de política e configurações de aplicativo locais aplicadas atualmente ao dispositivo.

Os perfis de política funcionam de acordo com as seguintes regras:

- Um perfil de política entra em vigor quando ocorre uma condição de ativação específica.
- Os perfis contêm valores de configurações que diferem das configurações de política.

- A ativação de um perfil de política altera as configurações em vigor do dispositivo gerenciado.
- Uma política pode incluir no máximo 100 perfis de política.

Não é possível criar uma política do Servidor de Administração.

Sobre as configurações de bloqueio e bloqueadas

Cada configuração de política tem um ícone de botão de bloqueio (). A tabela abaixo mostra os status do botão de bloqueio:

Status do botão de bloqueio

Status	Descrição
Indefinido	Se um cadeado aberto for exibido ao lado de uma configuração e o botão de alternância estiver desativado, a configuração não será especificada na política. Um usuário pode alterar essas configurações na interface gerenciada do aplicativo. Esse tipo de configuração é chamado de *desbloqueado*.
Aplicar	Se um cadeado fechado for exibido ao lado de uma configuração e o botão de alternância estiver ativado, a configuração será aplicada aos dispositivos nos quais essa política é aplicada. O usuário não pode modificar os valores dessas configurações na interface gerenciada do aplicativo. Esse tipo de configuração é chamado de *bloqueado*.

É altamente recomendável que você bloqueie as configurações da política que deseja aplicar nos dispositivos gerenciados. As configurações da política desbloqueadas podem ser reatribuídas pelas configurações do aplicativo da Kaspersky em um dispositivo gerenciado.

Você pode usar um botão de bloqueio para realizar as seguintes ações:

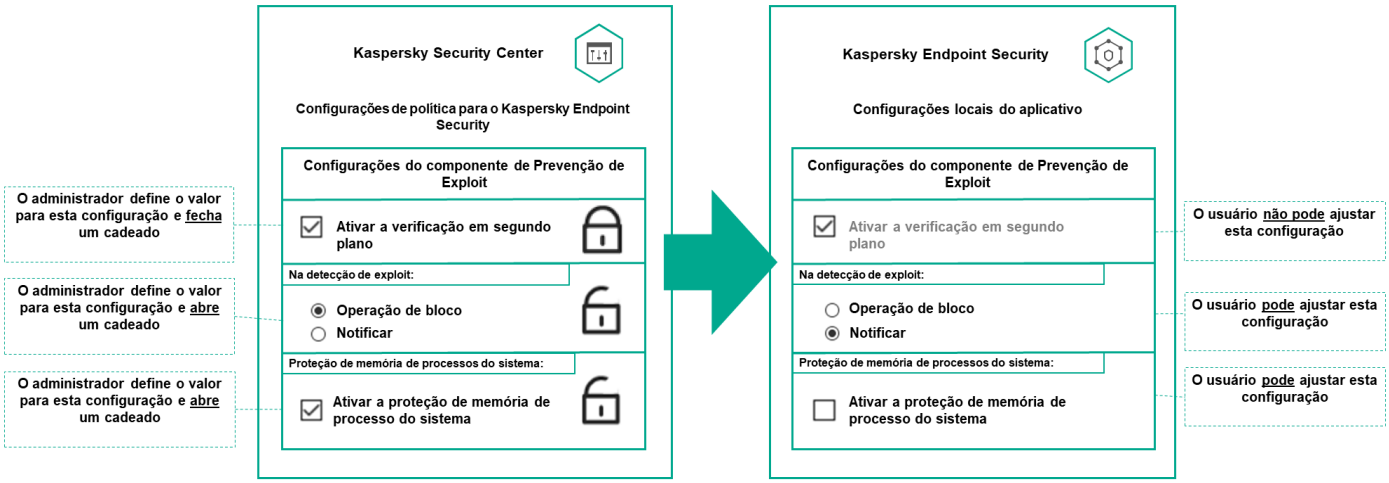
- Configurações de bloqueio para uma política de subgrupo de administração
- Bloqueando as configurações de um aplicativo da Kaspersky em um dispositivo gerenciado

Assim, uma configuração bloqueada é usada para implementar configurações efetivas em um dispositivo gerenciado.

Um processo de implementação de configurações eficazes inclui as seguintes ações:

- O dispositivo gerenciado aplica os valores de configuração do aplicativo da Kaspersky.
- O dispositivo gerenciado aplica valores de configurações bloqueados de uma política.

Uma política e um aplicativo da Kaspersky gerenciado contêm o mesmo conjunto de configurações. Ao definir as configurações de política, as configurações do aplicativo da Kaspersky mudam de valores em um dispositivo gerenciado. Não é possível ajustar as configurações bloqueadas em um dispositivo gerenciado (ver figura abaixo):



Configurações de bloqueio e de aplicativos da Kaspersky

Herança de políticas e perfis de política

Esta seção fornece informações sobre a hierarquia e herança de políticas e perfis de política.

Hierarquia de políticas

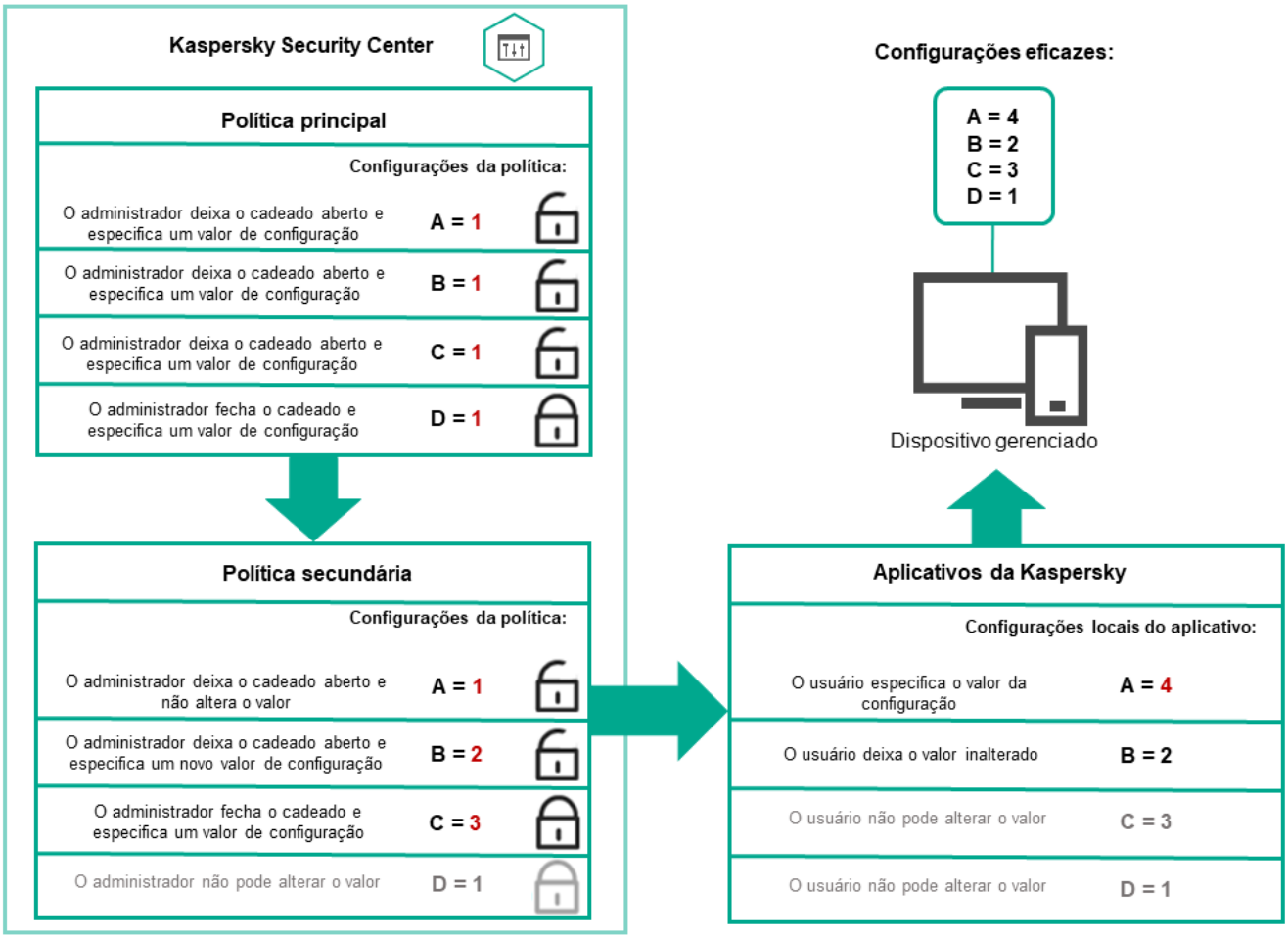
Se dispositivos diferentes precisarem de configurações diferentes, você pode organizar os dispositivos em grupos de administração.

Você pode especificar uma política para um único grupo de administração. As configurações de política podem ser *herdadas*. Herança significa receber valores de configurações de política em subgrupos (grupos secundários) de uma política de um grupo de administração de nível superior (principal).

Depois disso, a política de um grupo principal é também referida como uma *política principal*. Uma política para um subgrupo (grupo secundário) também é chamada de *política secundária*.

Por padrão, pelo menos um grupo de dispositivos gerenciados existe no Servidor de Administração. Se você deseja criar grupos personalizados, esses são criados como subgrupos (grupos secundários) dentro do grupo de dispositivos gerenciados.

Políticas de um mesmo aplicativo atuam entre si, de acordo com uma hierarquia de grupos de administração. As configurações bloqueadas de uma política de um grupo de administração de nível superior (principal) reatribuirão os valores das configurações de política de um subgrupo (ver figura abaixo).

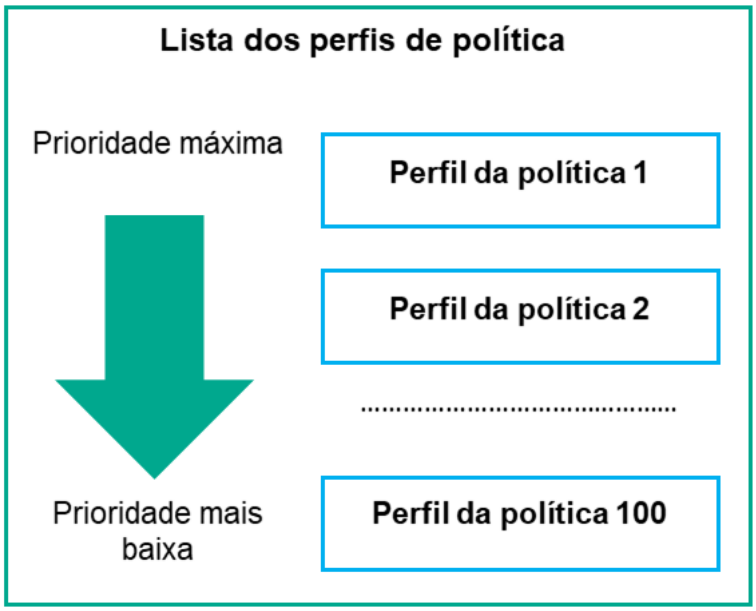


Hierarquia de políticas

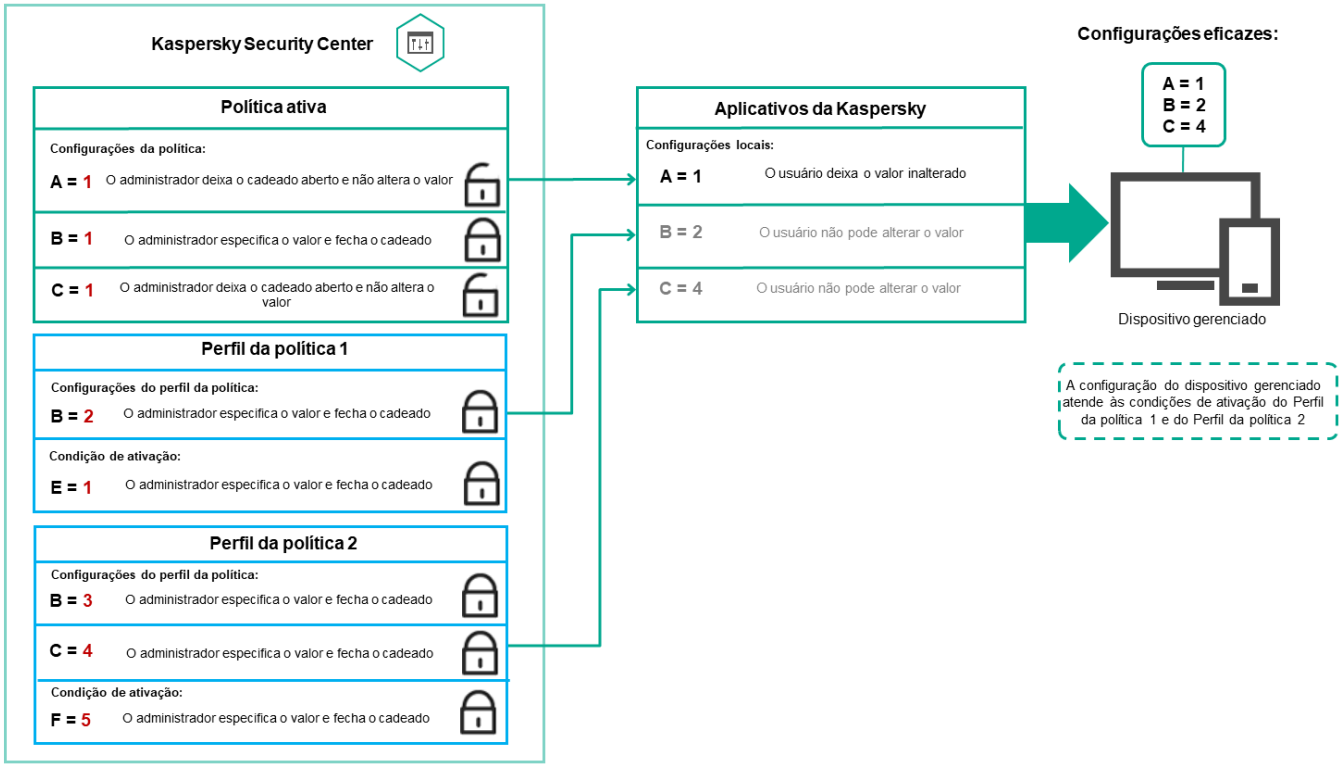
Perfis de política em uma hierarquia de políticas

Os perfis de política têm as seguintes condições de atribuição de prioridade:

- A posição de um perfil em uma lista de perfis de política indica sua prioridade. Você pode alterar uma prioridade de perfil da política. A posição mais alta em uma lista indica a prioridade mais alta (veja a figura abaixo).



- As condições de ativação dos perfis de política não dependem umas das outras. Vários perfis de política podem ser ativados simultaneamente. Se vários perfis de política afetam a mesma configuração, o dispositivo obtém o valor de configuração do perfil de política com a prioridade mais alta (veja a figura abaixo).



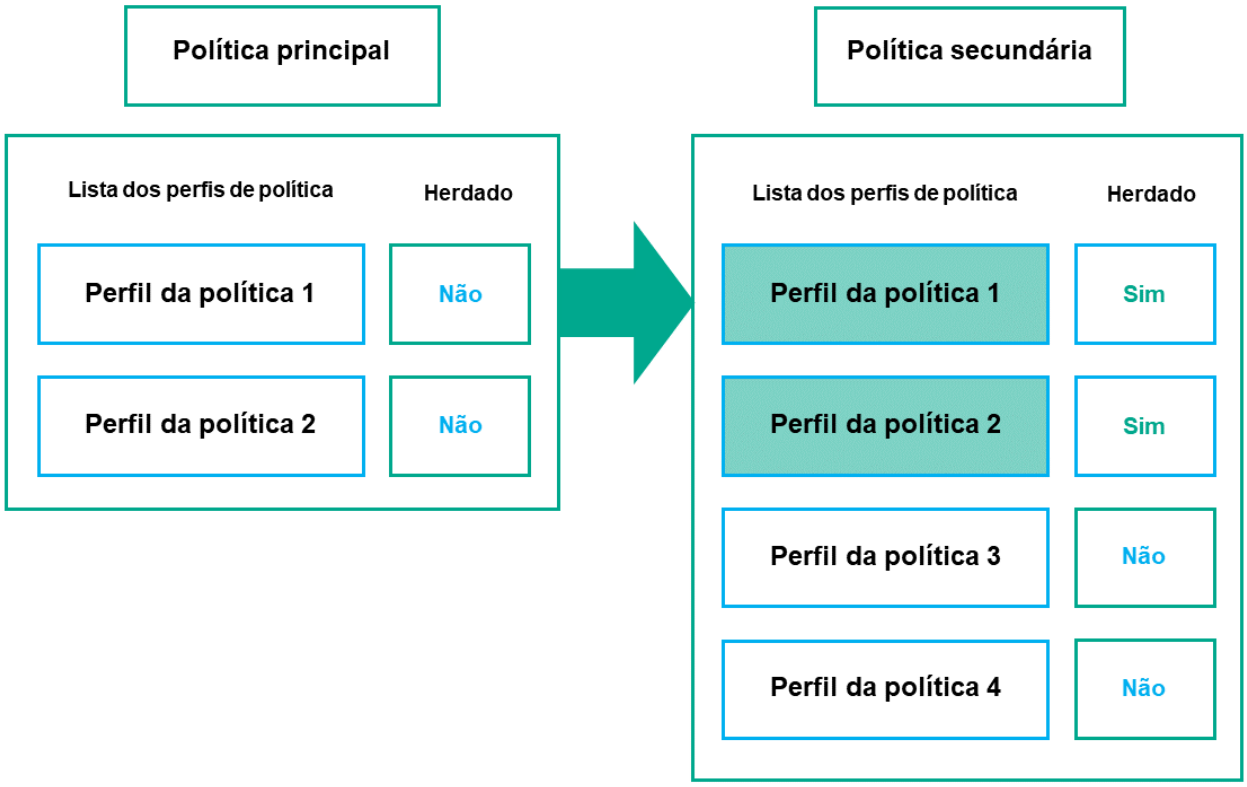
A configuração do dispositivo gerenciado atende às condições de ativação de vários perfis de política

Perfis de política em uma hierarquia de herança

Os perfis de política de diferentes políticas de nível de hierarquia estão em conformidade com as seguintes condições:

- Uma política de nível inferior herda perfis de política de uma política de nível superior. Um perfil de política herdado de uma política de nível superior obtém prioridade mais alta do que o nível do perfil de política original.

- Você não pode alterar a prioridade de um perfil de política herdado (veja a figura abaixo).

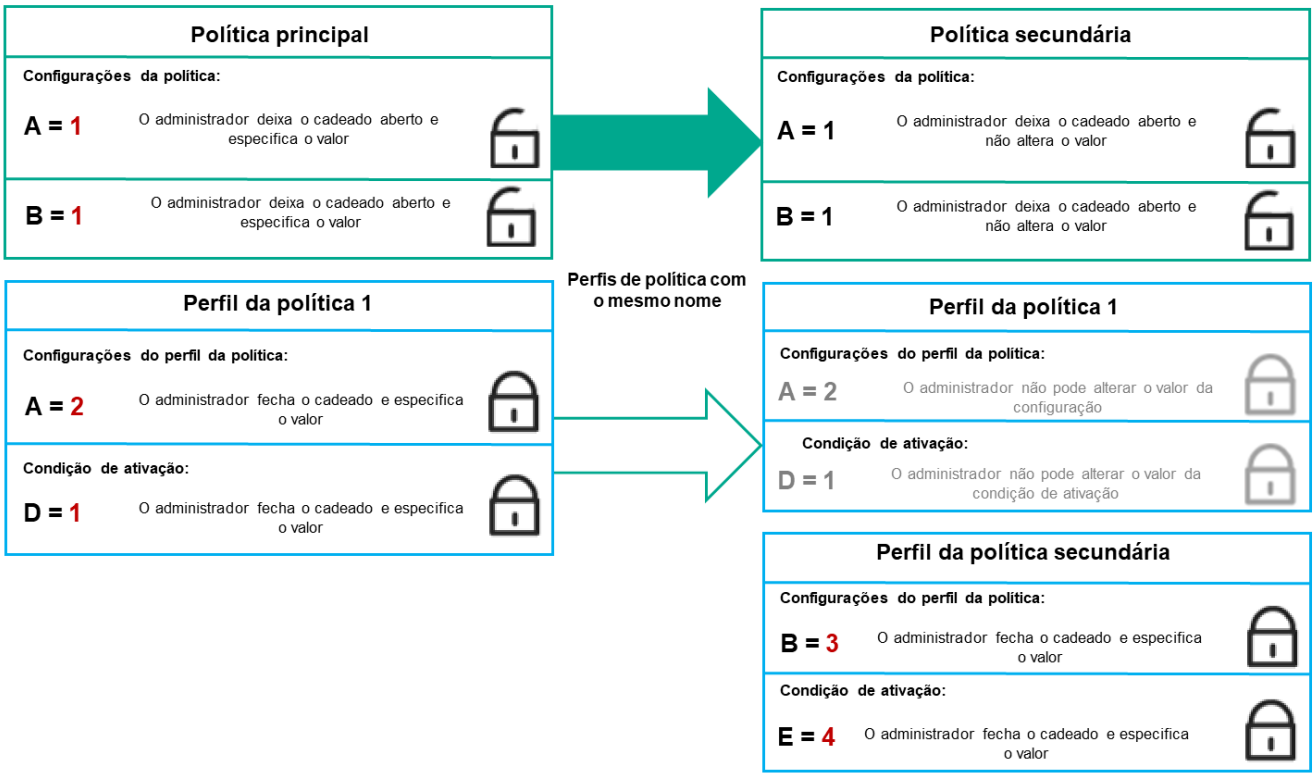


Herança de perfis de política

Perfis de política com o mesmo nome

Se houver duas políticas com o mesmo nome em diferentes níveis de hierarquia, essas funcionarão de acordo com as seguintes regras:

- As configurações bloqueadas e a condição de ativação de perfil de um perfil de política de nível superior alteram as configurações e a condição de ativação de perfil de um perfil de política de nível inferior (ver figura abaixo).



O perfil secundário herda os valores de configuração de um perfil de política principal

- As configurações desbloqueadas e a condição de ativação de perfil de um perfil de política de nível superior não alteram as configurações e a condição de ativação de perfil de um perfil de política de nível inferior.

Como as configurações são implementadas em um dispositivo gerenciado

A implementação eficaz de configurações em um dispositivo gerenciado pode ser descrita da seguinte forma:

- Os valores de todas as configurações não bloqueadas são obtidos a partir da política.
- Em seguida, são substituídos pelos valores das configurações do aplicativo gerenciado.
- Em seguida, os valores das configurações bloqueadas da política em vigor são aplicados. Os valores das configurações bloqueadas alteram os valores das configurações em vigor desbloqueadas.

Gerenciamento de políticas

Esta seção descreve o gerenciamento de políticas e fornece informações sobre como visualizar a lista de políticas, criar, modificar, copiar, mover políticas, sincronização forçada, visualizar o gráfico de status de distribuição de política e excluir uma política.

Visualização da lista de políticas

Você pode visualizar listas de políticas criadas para o Servidor de Administração ou para qualquer grupo de administração.

Para visualizar uma lista de políticas:

1. No menu principal, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Na estrutura de grupos de administração, selecione o grupo de administração para o qual você deseja exibir a lista de políticas.

A lista de políticas aparece em formato tabular. Se não houver políticas, a tabela ficará vazia. Você pode mostrar ou ocultar as colunas da tabela, modificar a sua ordem, exibir apenas linhas que contenham um valor especificado ou usar a pesquisa.

Criação de uma política

Você pode criar políticas; pode também modificar e excluir as políticas existentes.

Não é possível criar uma política do Servidor de Administração.

Para criar uma política:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique em **Adicionar**.

   A janela **Selecione o aplicativo** se abre.
3. Selecione o aplicativo para o qual você deseja criar uma política.
4. Clique em **Avançar**.

   A nova janela de configurações de política é exibida com a guia **Geral** selecionada.
5. Se quiser, altere o nome padrão, o status padrão e as configurações de herança padrão da política.
6. Clique na guia **Configurações do aplicativo**.

   Ou você pode clicar em **Salvar** e sair. A política aparecerá na lista de políticas, e você poderá editar as suas configurações depois.
7. Na guia **Configurações do aplicativo**, no painel esquerdo, selecione a categoria desejada e, no painel de resultados à direita, edite as configurações da política. Você pode editar as configurações da política em cada categoria (seção).

   As configurações variam de acordo com o aplicativo para o qual você está criando a política. Para mais detalhes, consulte:

   - Configuração do Servidor de Administração
   - Configurações de política do Agente de Rede
   - Documentação do Kaspersky Endpoint Security for Windows

Para detalhes sobre as configurações de outros aplicativos de segurança, consulte a documentação do aplicativo correspondente.

Ao editar as configurações, você pode clicar em **Cancelar** para cancelar a última operação.

8. Clique em **Salvar** para salvar a política.

A política será exibida na lista de políticas.

Modificar uma política

Para modificar uma política:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique na política que deseja modificar.

   A janela Propriedades da política será aberta.
3. Especifique as configurações gerais e as configurações do aplicativo para o qual a política está sendo criada. Para mais detalhes, consulte:

   - Configuração do Servidor de Administração
   - Configurações de política do Agente de Rede
   - Documentação do Kaspersky Endpoint Security for Windows

   Para detalhes sobre as configurações de outros aplicativos de segurança, consulte a documentação desse aplicativo.
4. Clique em **Salvar**.

As alterações feitas à política serão salvas nas propriedades da política e aparecerão na seção **Histórico de revisões**.

Configurações da política gerais

Geral

Na guia **Geral**, você pode modificar o status da política e especificar a herança das configurações da política:

- No bloco **Status da política**, você poderá selecionar um dos modos de política:
  - **Ativo**
  - **Fora do escritório**

Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

- Inativo

  Se esta opção estiver selecionada, a política é habilitada, mas continua armazenada na pasta **Políticas**. Se necessário, a política pode ser habilitada.

- No grupo de configurações **Herança de configurações**, você pode configurar a herança de política:

  - Herdar configurações da política principal

    Se esta opção estiver ativada, os valores das configurações de política são herdados da política de grupo de nível superior e, portanto são bloqueados.

    Por padrão, esta opção está ativada.

  - Forçar herança de configurações nas políticas secundárias

    Se esta opção estiver ativada, após a aplicação das alterações da política, as seguintes ações serão realizadas:

    - Os valores das configurações da política serão propagados às políticas de subgrupos de administração, ou seja, às políticas secundárias.
    - No bloco **Herança de configurações** da seção **Geral** na janela Propriedades de cada política secundária, a opção **Herdar configurações da política principal** será automaticamente ativada.

    Se a opção estiver ativada, as configurações das políticas secundárias são bloqueadas.

    Por padrão, esta opção está desativada.

Configuração de eventos

A guia **Configuração de eventos**, permite configurar o registro e a notificação de eventos. Os eventos são distribuídos por nível de importância nas seguintes guias:

- **Crítico**

  A seção **Crítico** não é exibida nas propriedades de política do Agente de Rede.

- **Falha funcional**
- **Advertência**
- **Informações**

Na cada seção, a lista de eventos exibe os tipos de eventos e o prazo de armazenamento de eventos padrão no Servidor de Administração (em dias). Clicar em um tipo de evento permite especificar as seguintes configurações:

- **Registro de eventos**

  Você pode especificar por quantos dias armazenar o evento e selecionar onde armazenar o evento:

  - **Armazenar no banco de dados do Servidor de Administração por (dias)**

- **Armazenar no log de eventos do SO no dispositivo**

- **Notificações de eventos**

  Você pode selecionar se deseja ser notificado sobre o evento por e-mail.

  Por padrão, as configurações de notificação especificadas na guia Propriedades do Servidor de Administração (como endereço do destinatário) são usadas. Se desejar, você pode alterar as configurações na guia **E-mail**.

Histórico de revisões

A guia **Histórico de revisões** permite visualizar a lista de revisões da política e reverter as alterações feitas na política, caso seja necessário.

Ativando o desativando uma opção de herança de política

Para ativar ou desativar a opção de herança em uma política:

1. Abra a política necessária.
2. Abra a guia **Geral**.
3. Ative ou desative a herança de política:

   - Se você ativar **Herdar configurações da política principal** em uma política secundária e um administrador bloquear algumas configurações na política principal, então você não poderá alterar essas configurações na política do grupo secundário.

   - Se você desativar **Herdar configurações da política principal** em uma política secundária, então você poderá alterar todas as configurações na política secundária, mesmo se algumas configurações estiverem bloqueadas na política principal.

   - Se você ativar **Forçar herança de configurações nas políticas secundárias** no grupo principal, isso ativará a opção **Herdar configurações da política principal** para cada política secundária. Nesse caso, você não pode desativar esta opção para nenhuma política secundária. Todas as configurações bloqueadas na política principal são herdadas por imposição nos grupos secundários, e você não pode alterar essas configurações nos grupos secundários.

4. Clique no botão **Salvar** para salvar as alterações ou clique no botão **Cancelar** para rejeitar as alterações.

Por padrão, a opção **Herdar configurações da política principal** está ativada para uma nova política.

Se uma política tiver perfis, todas as políticas secundárias herdarão esses perfis.

Cópia de uma política

Você pode copiar políticas de um grupo de administração para outro.

Para copiar uma política para outro grupo de administração:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.

2. Marque a caixa de seleção ao lado da política (ou políticas) que deseja copiar.

3. Clique no botão **Copiar**.

   No lado direito da tela, a árvore dos grupos de administração aparece.

4. Na árvore, selecione o grupo de destino, isto é, o grupo para o qual deseja copiar a política (ou políticas).

5. Clique no botão **Copiar** na parte inferior da tela.

6. Clique em **OK** para confirmar a operação.

A política (políticas) será copiada para o grupo de destino com todos os seus perfis. O status de cada política copiada no grupo de destino será **Inativo**. Você pode alterar o status para **Ativo** a qualquer momento.

Se uma política com um nome idêntico ao da política recém-movida já existir no grupo de destino, o nome da política recém-movida será expandido com o índice (<próximo número da sequência>), por exemplo: (1).

Mover uma política

Você pode mover políticas de um grupo de administração para outro. Por exemplo, você quer excluir um grupo, mas deseja usar as políticas dele para outro grupo. Nesse caso, você move a política do grupo antigo para o novo antes de excluir o antigo.

Para mover uma política para outro grupo de administração:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.

2. Marque a caixa de seleção ao lado da política (ou políticas) que deseja mover.

3. Clique no botão **Migrar**.

   No lado direito da tela, a árvore dos grupos de administração aparece.

4. Na árvore, selecione o grupo de destino, isto é, o grupo para o qual deseja mover a política (ou políticas).

5. Clique no botão **Migrar** na parte inferior da tela.

6. Clique em **OK** para confirmar a operação.

   Caso uma política não seja herdada do grupo de origem, ela será movida para o grupo de destino com todos os seus perfis. O status da política no grupo de destino é **Inativo**. Você pode alterar o status para **Ativo** a qualquer momento.

   Caso uma política seja herdada do grupo de origem, ela permanecerá no grupo de origem. Ela é copiada para o grupo de destino com todos os seus perfis. O status da política no grupo de destino é **Inativo**. Você pode alterar o status para **Ativo** a qualquer momento.

Se uma política com um nome idêntico ao da política recém-movida já existir no grupo de destino, o nome da política recém-movida será expandido com o índice (<próximo número da sequência>), por exemplo: (1).

Exportação de uma política

O Kaspersky Security Center Cloud Console permite salvar uma política, suas configurações e os perfis da política em um arquivo KLP. Você pode usar este arquivo KLP para importar a política salva tanto para o Kaspersky Security Center Windows quanto para o Kaspersky Security Center Linux.

Para exportar uma política:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Marque a caixa de seleção ao lado da política que deseja exportar.

   Você não pode exportar várias políticas ao mesmo tempo. Se selecionar mais de uma política, o botão **Exportar** será desabilitado.
3. Clique no botão **Exportar**.
4. Na janela **Salvar como** que abrir, especifique o nome e o caminho do arquivo de política. Clique no botão **Salvar**.

   A janela **Salvar como** é exibida apenas se você usar Google Chrome, Microsoft Edge ou Opera. Caso outro navegador seja usado, o arquivo da política será salvo automaticamente na pasta **Downloads**.

Importação de uma política

O Kaspersky Security Center Cloud Console permite importar uma política de um arquivo KLP. O arquivo KLP contém a política exportada, suas configurações e os perfis da política.

Para importar uma política:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no botão **Importar**.
3. Clique no botão **Procurar** para escolher um arquivo de política que você deseja importar.
4. Na janela aberta, especifique o caminho para o arquivo de política KLP e clique no botão **Abrir**. Observe que você pode selecionar apenas um arquivo de política.

   O processamento da política é iniciado.
5. Após o processamento com êxito da política, selecione o grupo de administração ao qual deseja aplicar a política.
6. Clique no botão **Concluir** para encerrar a importação da política.

A notificação com os resultados da importação é exibida. Se a política for importada com êxito, você poderá clicar no link **Detalhes** para visualizar as propriedades da política.

Após a importação com êxito, a política será exibida na lista de políticas. As configurações e os perfis da política também são importados. Independentemente do status da política selecionada durante a exportação, a política importada está inativa. Você pode alterar o status da política nas propriedades da política.

Se a política recém-importada tiver um nome idêntico ao de uma política existente, o nome da política importada será expandido com o índice **(<próximo número da sequência>)**, por exemplo: **(1)**, **(2)**.

Visualizar o gráfico de status de distribuição da política

No Kaspersky Security Center Cloud Console, você pode ver o status do aplicativo de política em cada dispositivo em um gráfico de status de distribuição de política.

Para analisar o status de distribuição da política em cada dispositivo:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Marque a caixa de seleção ao lado da política para a qual deseja visualizar o status de distribuição nos dispositivos.
3. No menu exibido, selecione o link **Distribuição**.

   A janela **Resultados de distribuição <Nome da política>** é aberta.
4. Na janela aberta **Distribuição de resultados <Nome da política>** a **Descrição de status (se disponível)** da política é exibida.

É possível alterar o número de resultados exibidos na lista com a distribuição da política. O número máximo de dispositivos é 100.000.

Para alterar o número de dispositivos exibidos na lista com os resultados de distribuição da política:

1. No menu principal, acesse as configurações da conta e selecione **Opções da interface**.
2. Em **Quantidade máxima de dispositivos exibidos nos resultados de distribuição de políticas**, insira o número de dispositivos (até 100.000).

   Por padrão, o número é 5.000.
3. Clique em **Salvar**.

As configurações são salvas e aplicadas.

Ativação automática de uma política no evento Ataque de vírus

Para fazer com que uma política execute a ativação automática no evento de um ataque de vírus:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.
2. Selecione a seção **Surto de vírus**.
3. No painel direito, clique no link **Configurar as políticas para ativar em caso de um evento de surto de vírus**.

   A janela **Ativação da política** se abre.
4. Na seção relacionada ao componente que detecta um surto de vírus, Antivírus para estações de trabalho e servidores de arquivos, Antivírus para servidores de e-mail ou Antivírus para defesa de perímetro, selecione o botão de opção ao lado da entrada desejada e clique em **Adicionar**.

Uma janela é aberta com o grupo de administração de **Dispositivos gerenciados**.

5. Clique no ícone do separador (>) ao lado de **Dispositivos gerenciados**.

   Uma hierarquia de grupos de administração e suas políticas é exibida.

6. Na hierarquia de grupos de administração e suas políticas, clique no nome de uma política ou políticas que são ativadas quando um surto de vírus é detectado.

   Para selecionar todas as políticas na lista ou em um grupo, marque a caixa de seleção ao lado do nome desejado.

7. Clique no botão **Salvar**.

   A janela com a hierarquia dos grupos de administração e suas políticas é fechada.

As políticas selecionadas são adicionadas à lista de políticas que são ativadas quando um surto de vírus é detectado. As políticas selecionadas são ativadas no surto de vírus, independentemente de estarem ativas ou inativas.

Se uma política tiver sido ativada no evento Ataque de vírus, você somente pode voltar à política anterior usando o modo manual.

Sincronização forçada

Embora o Kaspersky Security Center Cloud Console sincronize automaticamente o status, as configurações, as tarefas e as políticas para dispositivos gerenciados, em alguns casos e num dado momento, é necessário saber exatamente se a sincronização já foi executada para um dispositivo especificado.

Sincronizar um único dispositivo

Para forçar a sincronização entre o Servidor de Administração e um dispositivo gerenciado:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.

2. Clique no nome do dispositivo que deseja sincronizar com o Servidor de Administração.

   Uma janela de propriedades é exibida com a seção **Geral** selecionada.

3. Clique no botão **Forçar a sincronização**.

O aplicativo sincroniza o dispositivo selecionado com o Servidor de Administração.

Sincronizar vários dispositivos

Para forçar a sincronização entre o Servidor de Administração e vários dispositivos gerenciados:

1. Abra a lista de dispositivos de um grupo de administração ou uma seleção de dispositivos:

   - No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados** → **Grupos**, e selecione o grupo de administração que contém os dispositivos a serem sincronizados.

- Execute uma seleção de dispositivos para visualizar a lista de dispositivos.

2. Marque as caixas de seleção ao lado dos dispositivos que deseja sincronizar com o Servidor de Administração.

3. Clique no botão **Forçar a sincronização**.

   O aplicativo sincroniza os dispositivos selecionados com o Servidor de Administração.

4. Na lista de dispositivos, verifique se a hora da última conexão com o Servidor de Administração foi alterada para os dispositivos selecionados para a hora atual. Se a hora não tiver sido alterada, atualize o conteúdo da página clicando no botão **Atualizar**.

Os dispositivos selecionados são sincronizados com o Servidor de Administração.

Visualização da hora da entrega de uma política

Após alterar a política de um aplicativo da Kaspersky no Servidor de Administração, é possível verificar se a política alterada foi entregue a um dispositivo gerenciado específico. Uma política pode ser entregue durante uma sincronização normal ou uma sincronização forçada.

Para visualizar a data e a hora que uma política de aplicativo foi fornecida a um dispositivo gerenciado:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.

2. Clique no nome do dispositivo que deseja sincronizar com o Servidor de Administração.

   Uma janela de propriedades é exibida com a seção **Geral** selecionada.

3. Clique na guia **Aplicativos**.

4. Selecione o aplicativo do qual do qual deseja visualizar a data de sincronização da política.

A janela de política do aplicativo é exibida com a seção **Geral** selecionada e a data e a hora de entrega da política exibidas.

Exclusão de uma política

Você pode excluir uma política se não precisar mais dela. Você pode excluir apenas uma política que não é herdada no grupo de administração especificado. Se uma política for herdada, você só poderá exclui-la no grupo de nível superior para o qual ela foi criada.

Para excluir uma política:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.

2. Marque a caixa de seleção ao lado da política que deseja excluir e clique em **Excluir**.

   O botão **Excluir** ficará indisponível (esmaecido) se você selecionar uma política herdada.

3. Clique em **OK** para confirmar a operação.

A política é excluída em conjunto com todos os seus perfis.

Gerenciando perfis de política

Esta seção descreve o gerenciamento de perfis de política e fornece informações sobre como visualizá-los, alterar a prioridade, criar, modificar, copiar, criar uma regra de ativação e excluir perfis de política.

Visualização dos perfis de uma política

Para visualizar os perfis de uma política:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política cujos perfis deseja exibir.

   A janela de propriedades da política é exibida com a guia **Geral** selecionada.
3. Abra a guia **Perfis de política**.

A lista de perfis da política é exibida em formato tabular. Se a política não tiver perfis, uma tabela vazia será exibida.

Alteração de uma prioridade de perfil da política

Para alterar uma prioridade de perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.
2. Na guia **Perfis de política**, marque a caixa de seleção ao lado do perfil da política para o qual deseja alterar a prioridade.
3. Defina uma nova posição do perfil da política na lista clicando em **Priorizar** ou **Desprioritizar**.

   Quanto mais alto um perfil da política estiver localizado na lista, mais alta será sua prioridade.
4. Clique no botão **Salvar**.

A prioridade do perfil da política selecionado é alterada e aplicada.

Criar um perfil da política

Para criar um perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida. Se a política não tiver perfis, uma tabela vazia será exibida.

2. Clique em **Adicionar**.
3. Se quiser, altere o nome padrão e as configurações de herança padrão do perfil.
4. Selecione a guia **Configurações do aplicativo**.

   Ou então, é possível clicar em **Salvar** e sair. O perfil criado aparecerá na lista de perfis da política, e será possível editar as suas configurações depois.
5. Na guia **Configurações do aplicativo**, no painel esquerdo, selecione a categoria desejada e, no painel de resultados à direita, edite as configurações do perfil. Você pode editar as configurações do perfil da política em cada categoria (seção).

   Ao editar as configurações, você pode clicar em **Cancelar** para cancelar a última operação.
6. Clique em **Salvar** para salvar o perfil.

O perfil aparecerá na lista de perfis da política.

Modificar um perfil da política

A capacidade para editar um perfil da política somente está disponível para políticas do Kaspersky Endpoint Security for Windows.

Para modificar um perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.
2. Na guia **Perfis de política**, selecione o perfil da política que deseja modificar.

   A janela Propriedades do perfil da política será aberta.
3. Configure o perfil na janela de propriedades:

   - Se necessário, na guia **Geral**, altere o nome do perfil e ative ou desative o perfil.
   - Edite as regras de ativação de perfil.
   - Edite as configurações do aplicativo.

   Para detalhes sobre configurações de aplicativos de segurança, veja a documentação do aplicativo correspondente.
4. Clique em **Salvar**.

As configurações que você modificou serão aplicadas após o dispositivo ser sincronizado com o Servidor de Administração (se o perfil da política estiver ativo) ou após a regra de ativação ser acionada (se o perfil da política estiver inativo).

Copiar um perfil de política

Você pode copiar um perfil da política para política atual ou outra, por exemplo, se quiser ter perfis idênticos para políticas diferentes. Você também pode usar a cópia se quiser ter dois ou mais perfis que se diferenciam em apenas um pequeno número de configurações.

Para copiar um perfil de política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida. Se a política não tiver perfis, uma tabela vazia será exibida.

2. Na guia **Perfis de política**, selecione o perfil da política que deseja copiar.

3. Clique em **Copiar**.

4. Na janela exibida, selecione a política para a qual deseja copiar o perfil.

   É possível copiar um perfil da política para a mesma política ou uma política que você especificar.

5. Clique em **Copiar**.

   O perfil da política é copiado para a política que você selecionou. O perfil recentemente copiado adquire a prioridade mais baixa. Se você copiar o perfil para a mesma política, o nome do perfil recentemente copiado será expandido com o índice (), por exemplo: (1), (2).

Depois, você pode modificar as configurações do perfil, inclusive o nome e a prioridade dele; o perfil da política original não será modificado nesse caso.

Criar uma regra de ativação do perfil da política

Para criar uma regra de ativação do perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.

2. Na guia **Perfis de política**, clique no perfil da política para o qual é preciso criar uma regra de ativação.

   Se a lista de perfis da política estiver vazia, você pode criar um perfil da política.

3. Na guia **Regras de ativação**, clique no botão **Adicionar**.

   A janela com as regras de ativação do perfil da política é aberta.

4. Especifique um nome para a regra.

5. Selecione as caixas junto as condições que devem afetar a ativação do perfil da política que você estiver criando:

   - **Regras gerais para a ativação do perfil de política**

     Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo do status do modo offline de dispositivo, a regra para a conexão ao Servidor de Administração e as tags atribuídas ao dispositivo.

     Para esta opção, especifique na etapa seguinte:

- Status do dispositivo

  Define a condição da presença do dispositivo na rede:

  - **Online** – O dispositivo está na rede, portanto o Servidor de Administração está disponível.
  - **Offline** – O dispositivo está em uma rede externa, o que significa que o Servidor de Administração não está disponível.
  - **N/A** – O critério não será aplicado.

- A regra para conexão do Servidor de Administração está ativa neste dispositivo

  Escolha a condição de ativação do perfil da política (se a regra está ou não sendo executada) e selecione o nome da regra.

  A regra define o local de rede do dispositivo para conexão ao Servidor de Administração, cujas condições devem ser atendidas (ou não devem ser atendidas) para a ativação do perfil da política.

  Uma descrição da localização da rede de dispositivos para conexão a um Servidor de Administração pode ser criada ou configurada em uma regra de troca de Agente de Rede.

- **Regras para o proprietário do dispositivo específico**

  Para esta opção, especifique na etapa seguinte:

  - Proprietário do dispositivo

    Ative esta opção para configurar e ativar a regra para a ativação do perfil no dispositivo para seu proprietário. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

    - O dispositivo pertence ao proprietário especificado (sinal "=").
    - O dispositivo não pertence ao proprietário especificado (sinal "≠").

      Observe que a lista de usuários é filtrada e exibe os proprietários do dispositivo que são usuários internos.

      Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o proprietário do dispositivo se a opção estiver ativada. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

  - O proprietário do dispositivo está incluído em um grupo de segurança interno

Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pela associação do proprietário em um grupo de segurança interna do Kaspersky Security Center Cloud Console. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

- O proprietário do dispositivo é um membro do grupo de segurança especificado (sinal "=").
- O proprietário do dispositivo não é um membro do grupo de segurança especificado (sinal "≠").

  Observe que a lista de usuários é filtrada e exibe os proprietários do dispositivo que são usuários internos.

  Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar um grupo de segurança do Kaspersky Security Center Cloud Console. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- **Regras para especificações de hardware**

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo do volume de memória e do número de processadores lógicos.

  Para esta opção, especifique na etapa seguinte:

  - **Tamanho da RAM, em MB**

    Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pelo volume de RAM disponível naquele dispositivo. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

    - O tamanho da RAM do dispositivo é menos do que o valor especificado (sinal "<").
    - O tamanho de RAM de dispositivo é maior do que o valor especificado (sinal ">").

    Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o volume da RAM no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

  - **Número de processadores lógicos**

    Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pelo número de processadores lógicos nesse dispositivo. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

    - O número de processadores lógicos no dispositivo é menor do que ou igual ao valor especificado (sinal "<").
    - O número de processadores lógicos no dispositivo é maior do que ou igual ao valor especificado (sinal ">").

    Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o número de processadores lógicos no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- **Regras para atribuição de funções**

  Para esta opção, especifique na etapa seguinte:

  Ativar o perfil de política por função específica do proprietário do dispositivo

Selecione esta opção para configurar e ativar a regra da ativação do perfil no dispositivo, dependendo da função do proprietário. Adicione a função manualmente da lista de funções existentes.

Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados.

- **Regras para uso de tag**

  Marque esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo das tags atribuídas ao dispositivo. Você pode ativar o perfil da política para os dispositivos com ou sem tags selecionadas.

  Para esta opção, especifique na etapa seguinte:

  - **Tag**

    Na lista de tags, especifique uma regra para a inclusão do dispositivo no perfil da política, selecionando as caixas de seleção ao lado das tags relevantes.

    Você pode adicionar novas tags à lista inserindo-as no campo sobre a lista e clicando no botão **Adicionar**.

    O perfil da política inclui dispositivos com descrições que contêm todas as tags selecionadas. Se as caixas de seleção forem desmarcadas, o critério não é aplicado. Por padrão, estas caixas de seleção estão desmarcadas.

  - **Aplicar aos dispositivos sem tags especificadas**

    Ative esta opção se tiver de inverter a seleção de tags.

    Se esta opção estiver selecionada, o perfil da política inclui dispositivos com descrições que não contêm nenhuma das tags selecionadas. Se esta opção estiver desativada, o critério não é aplicado.

    Por padrão, esta opção está desativada.

- **Regras para uso do Active Directory**

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo da presença do dispositivo em uma unidade organizacional (UO) do Active Directory ou em uma associação do dispositivo (ou seu proprietário) em um grupo de segurança do Active Directory.

  Para esta opção, especifique na etapa seguinte:

  - **Associação do proprietário do dispositivo em um grupo de segurança do Active Directory**

    Se esta opção estiver ativada, o perfil da política será ativado no dispositivo cujo proprietário for um membro do grupo de segurança especificado. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

  - **Associação do dispositivo no grupo de segurança do Active Directory**

    Se esta opção estiver ativada, o perfil da política será ativado no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- A alocação do dispositivo está na unidade organizacional do Active Directory

  Se esta opção estiver ativada, o perfil da política será ativado no dispositivo que estiver incluído na unidade organizacional (OU) do Active Directory especificada. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado.

  Por padrão, esta opção está desativada.

O número de páginas adicionais do assistente depende das configurações que você seleciona no primeiro passo. Você pode modificar as regras de ativação do perfil da política em outro momento.

6. Verifique a lista dos parâmetros configurados. Se a lista estiver correta, clique em **Criar**.

O perfil será salvo. O perfil será ativado no dispositivo quando as regras de ativação forem acionadas.

As regras de ativação do perfil da política criadas para o perfil são exibidas nas propriedades do perfil da política na guia **Regras de ativação**. Você pode modificar ou remover qualquer regra de ativação do perfil da política.

Múltiplas regras de ativação podem ser acionadas simultaneamente.

Excluir um perfil de política

Para excluir um perfil de política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.

2. Na guia **Perfis de política**, marque a caixa de seleção ao lado do perfil de política que deseja excluir e clique em **Excluir**.

3. Na janela exibida, clique em **Excluir** novamente.

O perfil da política é excluído. Se a política for herdada por um grupo de nível mais baixo, o perfil permanecerá nesse grupo, mas se tornará o perfil da política desse grupo. Isso é feito para eliminar a alteração significativa nas configurações dos aplicativos gerenciados instalados nos dispositivos de grupos de nível mais baixo.

Criptografia e proteção de dados

A criptografia de dados reduz o risco de vazamentos não intencionais, caso seu laptop ou disco rígido seja roubado ou perdido, ou por acesso não autorizado por usuários e aplicativos.

Os seguintes aplicativos da Kaspersky são compatíveis com criptografia:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

Você pode mostrar ou ocultar alguns dos elementos da interface relacionados ao recurso de gerenciamento de criptografia usando as configurações da interface do usuário.

Criptografia de dados no Kaspersky Endpoint Security for Windows

É possível gerenciar a tecnologia de Criptografia de Unidade de Disco BitLocker em dispositivos que executam um sistema operacional Windows para servidores ou estações de trabalho.

Ao usar esses componentes do Kaspersky Endpoint Security for Windows, é possível, por exemplo, ativar ou desativar a criptografia, visualizar a lista de unidades criptografadas ou gerar e visualizar relatórios sobre criptografia.

Configure a criptografia definindo as políticas do Kaspersky Endpoint Security for Windows no Kaspersky Security Center Cloud Console. O Kaspersky Endpoint Security for Windows executa a criptografia e a descriptografia de acordo com a política ativa em vigor. Para obter instruções detalhadas sobre como configurar regras e uma descrição dos recursos de criptografia, veja a Ajuda do Kaspersky Endpoint Security for Windows.

Criptografia de dados no Kaspersky Endpoint Security for Mac

Você pode usar a criptografia FileVault em dispositivos que executam macOS. Ao trabalhar com o Kaspersky Endpoint Security for Mac, você pode ativar ou desativar essa criptografia.

Configure a criptografia definindo as políticas do Kaspersky Endpoint Security for Windows no Kaspersky Security Center Cloud Console. O Kaspersky Endpoint Security for Mac executa a criptografia e a descriptografia de acordo com a política ativa em vigor. Para obter uma descrição detalhada sobre os recursos de criptografia, veja a Ajuda do Kaspersky Endpoint Security for Mac.

Visualização da lista de unidades criptografadas

No Kaspersky Security Center Cloud Console, é possível visualizar detalhes sobre unidades criptografadas e dispositivos criptografados no nível da unidade. Após as informações de uma unidade serem descriptografadas, a unidade é automaticamente removida da lista.

Para exibir a lista de unidades criptografadas,

No menu principal, vá para **Operações** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.

Se a seção não estiver no menu, isso significa que ela está oculta. Nas configurações da interface do usuário, habilite a opção **Mostrar a criptografia e proteção de dados** para exibir a seção.

É possível exportar a lista de unidades criptografadas para um arquivo CSV ou TXT. Para fazer isso, clique no botão **Exportar para CSV** ou **Exportar para TXT**.

Criação e visualização de relatórios de criptografia

É possível gerar os seguintes relatórios:

- Relatório de status da criptografia dos dispositivos gerenciados. Este relatório fornece detalhes sobre a criptografia de dados de vários dispositivos gerenciados. Por exemplo, o relatório mostra o número de

dispositivos aos quais a política com regras de criptografia configuradas se aplica. Além disso, você pode descobrir, por exemplo, quantos dispositivos precisam ser reinicializados. Ele também contém informações sobre a tecnologia de criptografia e o algoritmo para cada dispositivo.

- Relatório de status da criptografia dos dispositivos de armazenamento em massa. Este relatório contém informações semelhantes ao relatório sobre o status de criptografia de dispositivos gerenciados, mas fornece dados apenas para dispositivos de armazenamento em massa e unidades removíveis.
- Relatório de direitos de acesso aos dispositivos criptografados. Este relatório mostra quais contas de usuário têm acesso a unidades criptografadas.
- Relatório de erros na criptografia de arquivos. Este relatório contém informações sobre os erros que ocorreram ao executar as tarefas de criptografia ou a descriptografia dos dados nos dispositivos.
- Relatório de bloqueio de acesso aos arquivos criptografados. Este relatório contém informações sobre como bloquear o acesso dos aplicativos aos arquivos criptografados. Este relatório será útil se um usuário ou aplicativo não autorizado tentar acessar arquivos ou unidades criptografadas.

É possível gerar qualquer relatório na seção **Monitoramento e relatórios → Relatórios**. Alternativamente, na seção **Operações → Criptografia e proteção de dados**, você pode gerar os seguintes relatórios de criptografia:

- Relatório de status da criptografia dos dispositivos de armazenamento em massa
- Relatório de direitos de acesso aos dispositivos criptografados
- Relatório de erros na criptografia de arquivos

*Para gerar um relatório de criptografia na seção **Criptografia e proteção de dados**:*

1. Certifique-se de ter ativado a opção **Mostrar a criptografia e proteção de dados** nas opções de interface.
2. No menu principal, vá para **Operações → Criptografia e proteção de dados**.
3. Abra a seção **Dispositivos criptografados** para gerar o relatório sobre o status de criptografia dos dispositivos de armazenamento em massa ou o relatório sobre os direitos de acesso aos dispositivos criptografados.
4. Clique no nome do relatório que deseja gerar.

A geração do relatório começa.

Concessão de acesso a uma unidade criptografada no modo offline

Um usuário pode solicitar acesso a um dispositivo criptografado, por exemplo, quando o Kaspersky Endpoint Security for Windows não estiver instalado no dispositivo gerenciado. Depois que você receber a solicitação, poderá criar um arquivo de chave de acesso e enviá-lo ao usuário. Todos os casos de uso e instruções detalhadas são fornecidas na Ajuda do Kaspersky Endpoint Security for Windows.

Para conceder acesso a uma unidade criptografada no modo offline:

1. Obtenha um arquivo de solicitação de acesso de um usuário (com a extensão FDERTC). Siga as instruções da Ajuda do Kaspersky Endpoint Security for Windows para gerar o arquivo no Kaspersky Endpoint Security for Windows.
2. No menu principal, vá para **Operações → Criptografia e proteção de dados → Dispositivos criptografados**.

Uma lista de unidades criptografadas é exibida.

3. Selecione a unidade à qual o usuário solicitou acesso.
4. Clique no botão **Permitir acesso ao dispositivo em modo offline**.
5. Na janela que se abre, selecione o plug-in correspondente ao aplicativo da Kaspersky usado para criptografar a unidade selecionada.

   Se uma unidade for criptografada com um aplicativo Kaspersky não compatível com o Kaspersky Security Center Cloud Console, use o Console de administração baseado no Microsoft Management Console para conceder o acesso offline.

6. Siga as instruções fornecidas na Ajuda do Kaspersky Endpoint Security for Windows (veja os blocos de expansão no final da seção).

Depois disso, o usuário aplica o arquivo recebido para acessar a unidade criptografada e ler os dados armazenados na unidade.

Usuários e funções dos usuários

Esta seção descreve usuários e funções de usuário e fornece instruções para criá-los e modificá-los, atribuir funções e grupos a usuários e associar perfis de política a funções.

Sobre as contas de usuário

O Kaspersky Security Center Cloud Console permite gerenciar contas de usuário e grupos de contas. O aplicativo é compatível com dois tipos de contas:

- Contas dos funcionários da organização. O Servidor de Administração obtém dados das contas desses usuários locais ao fazer a sondagem da rede da organização.
- Contas de usuários internos do Kaspersky Security Center Cloud Console. É possível criar contas de usuários internos no portal. As contas serão utilizadas apenas no Kaspersky Security Center Cloud Console.

Para exibir as tabelas de contas de usuário e grupos de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos**.
2. Selecione a guia **Usuários** ou **Grupos**.

A tabela de usuários ou grupos de segurança é aberta. Por padrão, a tabela aberta é filtrada pelas colunas **Sub-tipo** e **Tem funções atribuídas**. A tabela exibe usuários internos ou grupos que têm funções atribuídas.

Se quiser visualizar a tabela apenas com as contas de usuários locais, defina o critério do filtro **Sub-tipo** como **Local**.

Se você alternar para um Servidor de Administração secundário versão 14.2 ou anterior e, em seguida, abrir a lista de usuários ou grupos de segurança, a tabela aberta será filtrada somente pela coluna **Sub-tipo**. O filtro pela coluna **Tem funções atribuídas** não será aplicado por padrão. A tabela filtrada conterá todos os usuários internos ou grupos de segurança com a função atribuída e sem ela.

Adicionar uma conta de usuário interno

Caso queira, é possível adicionar usuários internos ao espaço de trabalho no portal. Depois de adicionar um usuário interno, é possível atribuir-lhe uma função no Kaspersky Security Center Cloud Console.

Sobre as funções dos usuários

A *função de usuário* (também mencionada como uma *função*) é um objeto que contém um conjunto de direitos e privilégios. Uma função pode ser associada às configurações de aplicativos da Kaspersky instalados em um dispositivo de usuário. É possível atribuir uma função a um conjunto de usuários ou a um conjunto de grupos de segurança em qualquer nível na hierarquia de grupos de administração, Servidores de Administração, ou em nível de objetos específicos.

Caso gerencie dispositivos por meio de uma hierarquia de Servidores de Administração, a qual inclui Servidores de Administração virtuais, observe que é possível criar, modificar ou excluir as funções de usuário somente do Servidor de Administração físico. Em seguida, é possível propagar as funções de usuário para os Servidores de Administração secundários, incluindo os virtuais.

Você pode associar funções de usuário a perfis da política. Se uma função for atribuída a um usuário, esse usuário receberá as configurações de segurança necessárias para desempenhar suas funções profissionais.

Uma função de usuário pode ser associada a usuários de dispositivos em um grupo de administração específico.

Escopo da função do usuário

O *escopo da função do usuário* é uma combinação de usuários e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

Vantagem de usar funções

Uma vantagem de usar funções é que você não precisa especificar configurações de segurança para cada um dos dispositivos gerenciados ou cada um dos usuários separadamente. O número de usuários e dispositivos em uma empresa pode ser bastante grande, mas o número de funções de trabalho diferentes que necessitam de configurações de segurança diferentes é consideravelmente menor.

Diferenças do uso de perfis da política

Os perfis da política são as propriedades da política criada para cada aplicativo da Kaspersky separadamente. Uma função é associada a muitos perfis de política criados para aplicativos diferentes. Por isso, a função é um método da união de configurações para um determinado tipo de usuário em um lugar.

Configurar direitos de acesso aos recursos do aplicativo. Controle de acesso baseado em função

O Kaspersky Security Center Cloud Console fornece meios de acesso baseado em função para os recursos do Kaspersky Security Center Cloud Console e aplicativos gerenciados da Kaspersky.

É possível configurar os direitos de acesso aos recursos do aplicativo para os usuários do Kaspersky Security Center Cloud Console de uma das seguintes maneiras:

- Configurando os direitos para cada usuário ou grupo de usuários individualmente.
- Criando funções de usuário padrão com um conjunto predefinido de direitos e atribuindo tais funções aos usuários dependendo do escopo de obrigações deles.

A aplicação de funções de usuário tem como objetivo simplificar e reduzir os procedimentos de rotina de configuração de direitos de acesso dos usuários aos recursos do aplicativo. Os direitos de acesso com em uma função são configurados de acordo com as tarefas "padrão" e o escopo de deveres do usuário.

As funções de usuários podem ter nomes que correspondem a suas finalidades respetivas. Você pode criar um número ilimitado de funções no aplicativo.

É possível usar as funções de usuário predefinidas com um conjunto de direitos já configurado ou criar novas funções e configurar os direitos necessários por conta própria.

Direitos de acesso aos recursos do aplicativo

A tabela abaixo exibe os recursos do Kaspersky Security Center Cloud Console com os direitos de acesso para gerenciar as tarefas, os relatórios e as configurações associadas, assim como executar as ações associadas do usuário.

Para executar as ações do usuário listadas na tabela, o usuário deve ter o direito especificado ao lado da ação.

Os direitos de **Leitura**, **Gravação** e **Execução** são aplicáveis a qualquer tarefa, relatório ou configuração. Além desses direitos, o usuário deve ter o direito de **Executar operações nas seleções de dispositivos** para gerenciar tarefas, relatórios ou configurações nas seleções de dispositivos.

> Todas as tarefas, relatórios, configurações e pacotes de instalação que estão faltando na tabela pertencem à área funcional **Recursos gerais: Funcionalidade básica**.

Direitos de acesso aos recursos do aplicativo

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório
Recursos gerais: **Gerenciamento de grupos de administração**	**Gravação**	• Adicionar dispositivo em um grupo de administração: **Gravação**	Nenhum	Nenhum

		• Excluir dispositivo a partir de um grupo de administração: **Gravação** • Adicionar um grupo de administração em outro grupo de administração: **Gravação** • Excluir um grupo de administração a partir de outro grupo de administração: **Gravação**		
Recursos gerais: **Acessar objetos independentemente de suas ACLs**	**Ler**	Obter acesso de leitura a todos os objetos: **Leitura**	Nenhum	Nenhum
Recursos gerais: **Funcionalidade básica**	• **Ler** • **Gravação** • **Executar** • **Executar operações nas seleções de dispositivos**	• Regras de migração de dispositivos (criar, modificar ou excluir) para o Servidor virtual: **Gravação**, **executar operações nas seleções de dispositivos** • Obter certificado personalizado de protocolo móvel (LWNGT): **Ler** • Definir certificado personalizado de protocolo móvel (LWNGT): **Gravar** • Obter a lista de rede definida por NLA: **Ler** • Adicionar, modificar ou excluir a lista de rede definida por NLA: **Gravação** • Ver lista de controle de acesso de grupos: **Ler** • Ver o log de eventos Kaspersky: **Leia**	• "Baixar atualizações no repositório do Servidor de Administração" • "Entregar relatórios" • "Distribuir pacote de instalação" • "Instalar aplicativos nos Servidores de Administração secundários remotamente"	• "Relatório do status de proteção" • "Relatório de ameaças" • "Relatório de dispositivos mais infectados" • "Relatório de status dos bancos de dados antivírus" • "Relatório de erros" • "Relatório de ataques de rede" • "Relatório resumido de aplicativos de proteção do sistema de e-mail instalados" • "Relatório resumido de aplicativos de defesa de

				perímetro instalados" • "Relatório resumido dos tipos de aplicativos instalados" • "Relatório de usuários de dispositivos infectados" • "Relatar problemas de segurança" • "Relatório de eventos" • "Relatório de atividade dos pontos de distribuição" • "Relatório de Servidores de Administração secundários" • "Relatório de eventos de Controle de Dispositivos" • "Relatório de vulnerabilidades • "Relatório de aplicativos proibidos" • "Relatório de Controle da Web" • "Relatório de status da criptografia de dispositivos gerenciados" • "Relatório de status da criptografia de dispositivos de

				armazenamento em massa" • "Relatório de erros de criptografia de arquivos" • "Relatório de bloqueio de acesso a dispositivos criptografados" • "Relatório de direitos de acesso a dispositivos criptografados" • "Relatório de permissões do usuário em vigor" • "Relatório de direitos"
Recursos gerais: **Objetos excluídos**	• **Ler** • **Gravação**	• Ver os objetos excluídos na Lixeira: **Ler** • Excluir objetos a partir da lixeira: **Gravação**	Nenhum	Nenhum
Recursos gerais: **Processamento de eventos**	• **Excluir eventos** • **Editar configurações de notificação de eventos** • **Alterar configurações de log de eventos** • **Gravação**	• Alterar configurações de registro de eventos: **Editar configurações de log de eventos** • Alterar configurações de notificação de eventos: **Editar configurações de notificação de eventos** • Excluir eventos: **Excluir eventos**	Nenhum	Nenhum

Recursos gerais: **Implementação de software da Kaspersky**	• **Gerenciar patches da Kaspersky** • **Ler** • **Gravação** • **Executar** • **Executar operações nas seleções de dispositivos**	Aprovar ou recusar a instalação do patch: **Gerenciar patches da Kaspersky**	Nenhum	• "Relatório de uso da chave de licença pelo Servidor de Administração virtual" • "Relatório de versões de software da Kaspersky" • "Relatório de aplicativos incompatíveis" • "Relatório de versões das atualizações dos módulos de software da Kaspersky" • "Relatório de implementação da proteção"
Recursos gerais: **gerenciamento de chaves de licença**	• **Exportar arquivo de chave** • **Gravação**	• Exportar arquivo de chave: **Exportar arquivo de chave** • Modificar as configurações de chave de licença do Servidor de Administração: **Gravação**	Nenhum	Nenhum
Recursos gerais: **gerenciamento de relatórios aplicado**	• **Ler** • **Gravação**	• Criar relatórios independentemente	Nenhum	Nenhum

		de suas ACLs: **Gravar** • Executar relatórios independentemente de suas ACLs: **Ler**		
Recursos gerais: **Hierarquia de Servidores de Administração**	**Configurar uma hierarquia de Servidores de Administração**	Registrar, atualizar ou excluir Servidores de Administração secundários: **Configurar a hierarquia de Servidores de Administração**	Nenhum	Nenhum
Recursos gerais: **Permissões do usuário**	**Modificar ACLs de objetos**	• Alterar as propriedades de "Segurança" de qualquer objeto: **Modificar ACLs de objetos** • Gerenciar funções de usuário: **Modificar ACLs de objetos** • Gerenciar usuários internos: **Alterar ACLs de objeto** • Gerenciar grupos de segurança: **Alterar ACLs de objeto** • Gerenciar codinomes: **Modificar ACLs de objetos**	Nenhum	Nenhum
Recursos gerais: **Servidores de Administração Virtuais**	• **Gerenciar Servidores de Administração virtuais** • **Ler** • **Gravação** • **Executar** • **Executar operações nas seleções de dispositivos**	• Obter uma lista de Servidores de Administração virtuais: **Ler** • Obter informações sobre o Servidor de Administração virtual: **Ler** • Criar, atualizar ou excluir um Servidor de Administração virtual: **Gerenciar Servidores de**	Nenhum	"Relatório de resultados da instalação de atualizações de software de terceiros"

		Administração Virtuais • Mover um Servidor de Administração virtual para outro grupo: **Gerenciar Servidores de Administração Virtuais** • Definir permissões de Servidor virtual de administração: **Gerenciar servidores de administração virtuais**		
Recursos gerais: gerenciamento de chave de criptografia	**Gravação**	Importar as chaves de criptografia: **Gravação**	Nenhum	Nenhum
Gerenciamento do sistema: **Conectividade**	• **Iniciar sessões RDP** • **Conectar-se a sessões RDP existentes** • **Iniciar tunelamento** • **Salvar arquivos de dispositivos na estação de trabalho do administrador** • **Ler** • **Gravação** • **Executar** • **Executar operações nas seleções de dispositivos**	• Criar sessão de compartilhamento de área de trabalho: **O direito de criar uma sessão de compartilhamento de área de trabalho** • Criar sessão RDP: **Conectar-se a sessões RDP existentes** • Criar túnel: **Iniciar o tunelamento** • Salvar lista de rede de conteúdo: **Salvar arquivos de dispositivos na estação de trabalho do administrador**	Nenhum	"Relatório de usuários dos dispositivos"
Gerenciamento do sistema: **Inventário de hardware**	• **Ler** • **Gravação**	• Obter ou exportar objeto de inventário de hardware: **Ler**	Nenhum	• "Relatório do registro de hardware"

	• **Executar** • **Executar operações nas seleções de dispositivos**	• Adicionar, definir ou excluir objeto de inventário de hardware: **Gravação**		• "Relatório de alterações de configuração" • "Relatório de hardware"
Gerenciamento do sistema: **Controle de acesso à rede**	• **Ler** • **Gravação**	• Ver as configurações CISCO: **Ler** • Alterar as configurações CISCO: **Gravação**	Nenhum	Nenhum
Gerenciamento do sistema: **Implementação do sistema operacional**	• **Implementar servidores PXE** • **Ler** • **Gravação** • **Executar** • **Executar operações nas seleções de dispositivos**	• Implementar servidores PXE: **Implementar servidores PXE** • Ver uma lista de servidores PXE: **Ler** • Iniciar ou interromper o processo de instalação em clientes PXE: **Executar** • Gerenciar drivers para WinPE e imagens do sistema operacional: **Gravação**	"Criar pacote de instalação mediante imagem do SO do dispositivo de referência"	Nenhum
Gerenciamento de sistema: **Gerenciamento de patches e vulnerabilidades**	• **Ler** • **Gravação** • **Executar** • **Executar operações nas seleções de dispositivos**	• Ver propriedades de patch de terceiros: **Ler** • Alterar propriedades de patch de terceiros: **Gravação**	• "Executar a sincronização com o Windows Update" • "Instalar atualizações do Windows Update" • "Corrigir vulnerabilidades" • "Instalar as atualizações necessárias e corrigir vulnerabilidades"	"Relatório de atualizações de software"

Gerenciamento do sistema: **Instalação remota**	• **Ler** • **Gravação** • **Executar** • **Executar operações nas seleções de dispositivos**	• Visualizar as propriedades do pacote de instalação com base em Gerenciamento de patches e vulnerabilidade de terceiros: **Ler** • Alterar as propriedades do pacote de instalação baseado em gerenciamento de patches e vulnerabilidade de terceiros: **Gravação**	Nenhum	Nenhum
Gerenciamento do sistema: **Inventário de software**	• **Ler** • **Gravação** • **Executar** • **Executar operações nas seleções de dispositivos**	Nenhum	Nenhum	• "Relatório de aplicativos instalados" • "Relatório do histórico de registro de aplicativos" • "Relatório de status dos grupos de aplicativos licenciados" • "Relatório de chaves de licença de software de terceiros"

Funções de usuário predefinidas

As funções de usuário atribuídas aos usuários do Kaspersky Security Center Cloud Console fornecem conjuntos de direitos de acesso aos recursos do aplicativo.

Os usuários criados em um servidor virtual não podem receber uma função no Servidor de Administração.

É possível usar as funções de usuário predefinidas com um conjunto de direitos já configurado ou criar novas funções e configurar os direitos necessários por conta própria. Algumas das funções de usuário predefinidas disponíveis no Kaspersky Security Center Cloud Console podem ser associadas a cargos específicos, por exemplo, **Auditor**, **Diretor de segurança**, **Supervisor** (essas funções estão presentes no Kaspersky Security Center Cloud Console a partir da versão 11). Os direitos de acesso dessas funções são pré-configurados de acordo com as tarefas padrão e o escopo das obrigações dos cargos associados. A tabela abaixo mostra como as funções podem ser associadas a cargos específicos.

Exemplos de funções para cargos específicos

Função	Comentário
Auditor	Permite todas as operações com todos os tipos de relatórios, todas as operações de visualização, inclusive a observação de objetos excluídos (concede as permissões **Leitura** e **Gravação** na área **Objetos excluídos**). Não permite outras operações. Você pode atribuir esta função a uma pessoa que realiza a auditoria da sua organização.
Supervisor	Permite a visualização de todas as operações; não permite outras operações. Você pode atribuir esta função a um diretor de segurança e a outros gerentes responsáveis pela segurança de TI em sua organização.
Diretor de segurança	Permite todas as operações de visualização, permite o gerenciamento de relatórios; concede permissões limitadas na área **Gerenciamento do sistema**: **Conectividade**. Você pode atribuir esta função a um diretor responsável pela segurança de TI em sua organização.

A tabela abaixo mostra os direitos de acesso atribuídos a cada função de usuário predefinida.

Direitos de acesso de funções de usuário predefinidas

Função	Descrição

Administrador do Servidor de Administração	Permite todas as operações nas seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Processamento de eventos**
	  • **Hierarquia de Servidores de Administração**
	  • **Servidores de Administração virtual**
	• **Gerenciamento do sistema**:
	  • **Conectividade**
	  • **Inventário de hardware**
	  • **Inventário de software**
	Concede os direitos de **Leitura** e **Gravação** na área funcional **recursos gerais: gerenciamento de chaves de criptografia**.

Operador do Servidor de Administração	Concede os direitos de **Ler** e **Executar** em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Servidores de Administração virtual**

	• **Gerenciamento do sistema**:
	  • **Conectividade**
	  • **Inventário de hardware**
	  • **Inventário de software**

Auditor	Permite todas as operações nas seguintes áreas funcionais, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Objetos excluídos** • **Gerenciamento de relatórios aplicado** Você pode atribuir esta função a uma pessoa que realiza a auditoria da sua organização.

Administrador de instalação	Permite todas as operações nas seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Implementação de software da Kaspersky**
	  • **Gerenciamento de chaves de licença**
	• **Gerenciamento do sistema**:
	  • **Implementação do sistema operacional**
	  • **Gerenciamento de patches e vulnerabilidades**
	  • **Instalação remota**
	  • **Inventário de software**
	Concede os direitos de **Ler** e **Executar** na área funcional **Recursos gerais: Servidores de Administração Virtuais**.

Operador de instalação	Concede os direitos de **Ler** e **Executar** em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Implementação de software Kaspersky** (também concede o direito de **Gerenciar patches da Kaspersky** nesta área)
	  • **Servidores de Administração virtual**
	• **Gerenciamento do sistema**:
	  • **Implementação do sistema operacional**
	  • **Gerenciamento de patches e vulnerabilidades**

	• **Instalação remota** • **Inventário de software**
Administrador do Kaspersky Endpoint Security	Permite todas as operações nas seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • Área do Kaspersky Endpoint Security, incluindo todos os recursos Concede os direitos de **Leitura** e **Gravação** na área funcional **recursos gerais: gerenciamento de chaves de criptografia**.
Operador do Kaspersky Endpoint Security	Concede os direitos de **Ler** e **Executar** em todas as seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • Área do Kaspersky Endpoint Security, incluindo todos os recursos
Administrador Principal	Permite todas as operações em áreas funcionais, *exceto* as seguintes áreas, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Gerenciamento de relatórios aplicado** Concede os direitos de **Leitura** e **Gravação** na área funcional **recursos gerais: gerenciamento de chaves de criptografia**.

Operador Principal	Concede os direitos de **Ler** e **Executar** (quando aplicável) em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Objetos excluídos**
	  • **Operações no Servidor de Administração**
	  • **Implementação do software da Kaspersky**
	  • **Servidores de Administração virtual**
	• **Gerenciamento de Dispositivos Móveis: Geral**
	• **Gerenciamento do sistema**, incluindo todos os recursos
	• Área do Kaspersky Endpoint Security, incluindo todos os recursos

Administrador do Gerenciamento de Dispositivos Móveis	Permite todas as operações nas seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • **Gerenciamento de Dispositivos Móveis: Geral**
Operador do Gerenciamento	Concede os direitos de **Ler** e **Executar** na área funcional **Recursos gerais: Funcionalidade básica**.

de Dispositivos Móveis	Concede os comandos **Ler** e **Enviar somente informações para dispositivos móveis** na área funcional **Gerenciamento de dispositivos móveis**: **Geral**.
Diretor de segurança	Permite todas as operações nas seguintes áreas funcionais, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Gerenciamento de relatórios aplicado** Concede os direitos de **Leitura**, **Gravação**, **Execução**, **e Salvamento dos arquivos dos dispositivos na estação de trabalho do administrador** e **executar operações nas seleções de dispositivos** na área funcional **gerenciamento do sistema: conectividade**. Você pode atribuir esta função a um diretor responsável pela segurança de TI em sua organização.
Analista de segurança sênior	Concede os direitos de **Leitura** nos **Recursos gerais**: na área funcional **Funcionalidade básica**. Concede os direitos de **Leitura**, **Gravação**, **Execução**, **Salvamento dos arquivos dos dispositivos na estação de trabalho do administrador** e **Execução de operações nas seleções de dispositivos** na área funcional **Gerenciamento do sistema: Conectividade**. Concede os direitos de acesso à solução Kaspersky Endpoint Detection and Response Expert.
Usuário do Self Service Portal	Permite todas as operações na área funcional **Gerenciamento de Dispositivos Móveis: Self Service Portal**. Esse recurso não é compatível com o Kaspersky Security Center 11 e versões posteriores.
Supervisor	Concede o direito de **Leitura** nas áreas funcionais **Recursos gerais**: **Acessar objetos independentemente de suas ACLs** e **Recursos gerais**: **Gerenciamento de relatórios aplicado**. Você pode atribuir esta função a um diretor de segurança e a outros gerentes responsáveis pela segurança de TI em sua organização.
Administrador de gerenciamento de patches e vulnerabilidades	Permite todas as operações nas áreas funcionais **Recursos gerais**: **Funcionalidade básica** e **Gerenciamento do sistema** (incluindo todos os recursos).
Operador de gerenciamento de patches e vulnerabilidades	Concede os direitos de **Ler** e **Executar** (quando aplicável) nas áreas funcionais **Recursos gerais**: **Funcionalidade básica** e **Gerenciamento do sistema** (incluindo todos os recursos).

Atribuição de direitos de acesso a objetos específicos

Além de atribuir direitos de acesso no nível do servidor, é possível configurar o acesso a objetos específicos, por exemplo, a uma tarefa específica. O aplicativo permite especificar direitos de acesso aos seguintes tipos de objetos:

- Grupos de administração
- Tarefas
- Relatórios

- Seleções de dispositivos
- Seleções de eventos

Para atribuir direitos de acesso a um objeto específico:

1. Dependendo do tipo de objeto, no menu principal, vá para a seção correspondente:
   - **Ativos (dispositivos) → Hierarquia de grupos**
   - **Ativos (dispositivos) → Tarefas**
   - **Monitoramento e relatórios → Relatórios**
   - **Ativos (dispositivos) → Seleções de dispositivos**
   - **Monitoramento e relatórios → Seleções de eventos**
2. Abra as propriedades do objeto para o qual deseja configurar os direitos de acesso.

   Para abrir a janela de propriedades de um grupo de administração ou de uma tarefa, clique no nome do objeto. As propriedades de outros objetos podem ser abertas usando o botão na barra de ferramentas.
3. Na janela de propriedades, abra a seção **Direitos de acesso**.

   A lista de usuários é aberta. Os usuários e grupos de segurança listados têm direitos de acesso ao objeto. Por padrão, se você usar uma hierarquia de grupos de administração ou Servidores, a lista e os direitos de acesso serão herdados do grupo de administração principal ou do Servidor principal.
4. Para poder modificar a lista, ative a opção **Usar permissões personalizadas**.
5. Configure os direitos de acesso:
   - Use os botões **Adicionar** e **Excluir** para modificar a lista.
   - Especifique os direitos de acesso para um usuário ou grupo de segurança. Execute uma das seguintes ações:
     - Caso queira especificar os direitos de acesso manualmente, selecione o usuário ou grupo de segurança, clique no botão **Direitos de acesso** e, em seguida, especifique os direitos de acesso.
     - Caso queira atribuir uma função de usuário ao usuário ou grupo de segurança, selecione o usuário ou grupo de segurança, clique no botão **Funções** e, em seguida, selecione a função a ser atribuída.
6. Clique no botão **Salvar**.

Os direitos de acesso ao objeto são configurados.

Atribuição de uma função a um usuário ou grupo de segurança

Para atribuir uma função a um usuário ou grupo de segurança:

1. No menu principal, vá para **Usuários e funções → Usuários e grupos** e selecione a guia **Usuários** ou **Grupos**.

2. Selecione o nome do usuário ou grupo de segurança a quem deseja atribuir uma função.

   É possível selecionar múltiplos nomes.

3. Na linha do menu, clique no botão **Atribuir função**.

   O Assistente de Atribuição de Funções é iniciado.

4. Siga as instruções do assistente: selecione a função que deseja atribuir aos usuários selecionados ou grupos de segurança e selecione o escopo da função.

   O *escopo da função do usuário* é uma combinação de usuários e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

A função com um conjunto de direitos para trabalhar com o Servidor de Administração será atribuída ao usuário (ou aos usuários ou ao grupo de segurança). Na lista de usuários ou grupos de segurança, uma caixa de seleção aparece na coluna **Tem funções atribuídas**.

Criar uma função de usuário

Para criar uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique em **Adicionar**.
3. Na janela **Nome da nova função** exibida, digite o nome da nova função.
4. Clique em **OK** para aplicar as alterações.
5. Na janela de propriedades da função exibida, altere as configurações da função:
   - Na guia **Geral**, edite o nome da função.

     Você não pode editar o nome de uma função predefinida.
   - Na guia **Configurações**, edite o escopo da função e as políticas e os perfis associados à função.
   - Na guia **Direitos de acesso**, edite os direitos de acesso a aplicativos da Kaspersky.
6. Clique em **Salvar** para salvar as alterações.

A nova função aparece na lista de funções de usuário.

Editar os direitos de acesso de um usuário

É possível editar os direitos de acesso do usuário para os seguintes objetos:

- Servidor de Administração
- Grupo de administração

- Tarefa
- Relatório
- Seleção de eventos
- Seleção de dispositivos

Para editar os direitos de acesso de um usuário:

1. Acesse a guia **Direitos de acesso** do objeto selecionado.
2. Selecione um usuário para o qual deseja editar os direitos de acesso.

   Caso selecione sua própria conta de usuário, não será possível revogar os próprios direitos de acesso. A alterações não serão salvas.

3. Clique no botão **Direitos de acesso**.
4. Na janela aberta, edite os direitos de acesso do usuário selecionado.
5. Clique no botão **OK**.

Os direitos de acesso para esse usuário foram alterados.

Editar uma função de usuário

Para editar uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função que deseja editar.
3. Na janela de propriedades da função exibida, altere as configurações da função:
   - Na guia **Geral**, edite o nome da função.
     Você não pode editar o nome de uma função predefinida.
   - Na guia **Configurações**, edite o escopo da função e as políticas e os perfis associados à função.
   - Na guia **Direitos de acesso**, edite os direitos de acesso a aplicativos da Kaspersky.
4. Clique em **Salvar** para salvar as alterações.

A função atualizada aparece na lista de funções de usuário.

Editar o escopo de uma função de usuário

O *escopo da função do usuário* é uma combinação de usuários e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

Para adicionar usuários, grupos de usuários e grupos de administração ao escopo de uma função de usuário, você pode usar qualquer dos seguintes métodos:

Método 1:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e selecione a guia **Usuários** ou **Grupos**.
2. Marque as caixas de seleção ao lado dos usuários e dos grupos de usuários que deseja adicionar ao escopo da função de usuário.
3. Clique no botão **Atribuir função**.

   O Assistente de Atribuição de Funções é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
4. Na página **Selecionar função** do assistente, selecione a função de usuário que deseja atribuir.
5. Na página **Definir escopo** do assistente, selecione o grupo de administração que deseja adicionar ao escopo da função de usuário.
6. Clique no botão **Atribuir função** para fechar a janela.

Os usuários ou os grupos de usuários selecionados e o grupo de administração selecionado são adicionados ao escopo da função de usuário.

Método 2:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função para a qual deseja definir o escopo.
3. Na janela de propriedades da função exibida, selecione a guia **Configurações**.
4. Na seção **Escopo da função**, clique em **Adicionar**.

   O Assistente de Atribuição de Funções é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
5. Na página **Definir escopo** do assistente, selecione o grupo de administração que deseja adicionar ao escopo da função de usuário.
6. Na página **Selecionar usuários** do assistente, selecione os usuários e os grupos de usuários que deseja adicionar ao escopo da função de usuário.
7. Clique no botão **Atribuir função** para fechar a janela.
8. Feche a janela propriedades da função.

Os usuários ou os grupos de usuários selecionados e o grupo de administração selecionado são adicionados ao escopo da função de usuário.

Excluir uma função de usuário

Para excluir uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Marque a caixa de seleção ao lado do nome da função que deseja excluir.
3. Clique em **Excluir**.
4. Na janela que se abre, clique em **OK**.

A função de usuário é excluída.

Associação de perfis da política a funções

Você pode associar funções de usuário a perfis da política. Nesse caso, a regra de ativação desse perfil da política é baseada na função: o perfil da política fica ativo para um usuário com a função especificada.

Por exemplo, a política proíbe qualquer software de navegação de GPS em todos os dispositivos em um grupo de administração. O software de navegação de GPS é necessário em um dispositivo único no grupo de administração de Usuários, notadamente que for de propriedade do courier. Nesse caso, você pode atribuir uma função "Courier" ao seu proprietário e criar um perfil da política, permitindo que o software de navegação de GPS seja executado apenas nos dispositivos a cujos proprietários é atribuída a função "Courier". Todas as outras configurações de política são preservadas. Somente o usuário com a função "Courier" poderá executar o software de navegação de GPS. Depois, se outro funcionário receber a função "Courier", o novo funcionário também poderá executar o software de navegação no dispositivo da sua organização. Executar o software de navegação de GPS ainda será proibido em outros dispositivos no mesmo grupo de administração.

Para associar uma função a um perfil da política:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função que deseja associar a um perfil da política.
   A janela de propriedades da função é exibida com a guia **Geral** selecionada.
3. Selecione a guia **Configurações** e role para baixo até a seção **Políticas e perfis**.
4. Clique em **Editar**.
5. Para associar a função a:
   - **Um perfil da política existente** – Clique no ícone de insígnia (>) ao lado do nome de política necessário e marque a caixa de seleção ao lado do perfil ao qual você deseja associar a função.
   - **Um novo perfil da política**:
     a. Marque a caixa de seleção ao lado da política para a qual deseja criar um perfil.
     b. Clique em **Novo perfil de política**.

c. Especifique um nome para o novo perfil e defina as configurações de perfil.

d. Clique no botão **Salvar**.

e. Selecione a caixa de seleção junto ao novo perfil.

6. Clique em **Atribuir à função**.

O perfil é associado à função e aparece nas propriedades da função. O perfil se aplica automaticamente a qualquer dispositivo cujo proprietário seja atribuído à função.

Criação de um grupo de segurança

Para criar um grupo de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e selecione a guia **Grupos**.
2. Clique em **Novo grupo**.
3. Na janela **Novo grupo**, especifique as seguintes configurações para o novo grupo de segurança:
   - **Nome**
   - **Descrição**
4. Clique em **OK** para salvar as alterações.

Um novo grupo de segurança é adicionado à lista de grupos de segurança.

Edição de um grupo de segurança

Para editar um grupo de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Grupos**.
2. Clique no nome do grupo de segurança que deseja editar.
3. Na janela de configurações do grupo que é aberta, altere as configurações do grupo de segurança:
   - Na guia **Geral**, é possível alterar as configurações de **Nome** e **Descrição**. Essas configurações estão disponíveis somente para os grupos de segurança internos.
   - Na guia **Usuários**, é possível adicionar usuários ao grupo de segurança. Essa configuração está disponível somente para usuários internos e grupos de segurança internos.
   - Na guia **Funções**, é possível atribuir uma função ao grupo de segurança.
4. Clique em **Salvar** para salvar as alterações.

As alterações são aplicadas ao grupo de segurança.

Adicionar as contas de usuário em um grupo interno

Você somente pode adicionar contas de usuários internos em um grupo interno.

Para adicionar as contas de usuários em um grupo interno:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e selecione a guia **Usuários**.
2. Marque as caixas de seleção ao lado das contas de usuário que deseja adicionar a um grupo.
3. Clique no botão **Atribuir grupo**.
4. Na janela **Atribuir grupo** exibida, selecione o grupo ao qual deseja adicionar contas de usuário.
5. Clique no botão **Atribuir**.

As contas de usuário são adicionadas ao grupo. Você também pode adicionar usuários internos a um grupo usando as configurações de grupo.

Excluindo um grupo de segurança

Você pode excluir apenas grupos de segurança internos.

Para excluir um grupo de usuários:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e selecione a guia **Grupos**.
2. Marque a caixa de seleção ao lado do grupo de usuários que deseja excluir.
3. Clique em **Excluir** e confirme a exclusão na janela que se abre.

O grupo de usuários é excluído.

Configurando a integração ADFS

Para permitir que os usuários registrados no Active Directory (AD) em sua organização entrem no Kaspersky Security Center Cloud Console, você deve configurar a integração com os Serviços de Federação do Active Directory (ADFS).

O Kaspersky Security Center Cloud Console é compatível com ADFS 3 (Windows Server 2016) ou uma versão posterior.

Para alterar as configurações de integração ADFS, você deve ter direito de acesso para alterar as permissões do usuário.

Antes de continuar, certifique-se de ter concluído a sondagem do Active Directory.

Para configurar a integração ADFS:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações de integração ADFS**.

3. Copie a URL de callback.

   Você precisa dessa URL para configurar a integração no Console de Gerenciamento ADFS.

4. No Console de Gerenciamento ADFS, adicione um novo grupo de aplicativos. Depois, adicione um novo aplicativo, selecionando o modelo **Server application** (os nomes dos elementos da interface da Microsoft são fornecidos em inglês).

   O console de gerenciamento ADFS gera a ID de cliente para o novo aplicativo. Você precisa da ID do cliente para configurar a integração no Kaspersky Security Center Cloud Console.

5. Como um URI de redirecionamento, especifique a URL de callback copiada na janela de propriedades do Servidor de Administração.

6. Gere um segredo do cliente. Você precisa do segredo do cliente para configurar a integração no Kaspersky Security Center Cloud Console.

7. Salve as propriedades do aplicativo adicionado.

8. Adicione um novo aplicativo ao grupo de aplicativos criado. Desta vez, selecione o modelo de **API da web**.

9. Na guia **Identificadores**, para a lista **Identificadores de partes confiáveis**, adicione a ID do cliente do aplicativo de servidor adicionado antes.

10. Na guia **Permissões de cliente**, na lista **Escopos permitidos**, selecione os escopos **allatclaims** e **openid**.

11. Na guia **Regras de Transformação de Emissão**, adicione uma nova regra selecionando o modelo **Enviar atributos LDAP como declarações**:

    a. Dê um nome à regra. Por exemplo, você pode chamá-ao de 'SID de grupo'.

    b. Selecione **Active Directory** como um armazenamento de atributos e, em seguida, mapear **Grupos de Token como SIDs** como um atributo LDAP para 'SID de Grupo' como um tipo de declaração de saída.

12. Na guia **Regras de Transformação de Emissão**, adicione uma nova regra selecionando o modelo **Enviar reivindicações usando uma regra personalizada**:

    a. Dê um nome à regra. Por exemplo, você pode chamá-la de 'ActiveDirectoryUserSID'.

    b. No campo **Regra personalizada** digite:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
";objectSID;{0}", param = c.Value);
```

13. No Kaspersky Security Center Cloud Console, abra novamente a seção **Configurações de integração ADFS**.

14. Ative o botão de alternância para a posição **Integração ADFS Ativada**.

15. Clique no link **Configurações** e especifique o arquivo contendo o certificado ou vários certificados para o servidor de federação.

16. Clique no link **Configurações de integração ADFS** e especifique as seguintes configurações:

    - URL do emissor

      O endereço de URL do servidor de federação operando em sua organização.

      Em particular, o Kaspersky Security Center Cloud Console adiciona '/.well-known/openid-configuration' ao endereço URL do emissor e tenta abrir o endereço de URL resultante (issuer_URL/.well-known/openid-configuration) para descobrir a configuração do emissor automaticamente.

    - ID do cliente

      ID do cliente que o servidor de federação gera para identificar o Kaspersky Security Center Cloud Console. Você pode encontrar a ID do cliente no Console de Gerenciamento ADFS na janela de propriedades do aplicativo do servidor que corresponde ao Kaspersky Security Center Cloud Console.

    - Segredo do cliente

      Você gera um segredo de cliente no Console de Gerenciamento ADFS ao especificar as propriedades do aplicativo de servidor que correspondem ao Kaspersky Security Center Cloud Console.

    - Domínio para autenticar usuários de

      Os membros do domínio selecionados poderão entrar no Kaspersky Security Center Cloud Console com suas credenciais de conta de domínio. Os nomes de domínio aparecem na lista depois de concluir a sondagem de rede.

    - Nome do campo para SID do usuário no token de ID

      Nome do campo referente à SID do usuário no token de ID. O nome do campo é necessário para identificar o usuário no Kaspersky Security Center Cloud Console. Por padrão, este campo no token de ID é denominado 'primarysid'.

    - Nome do campo para arranjo de SIDs dos grupos de usuários no token de ID

      Nome do campo referente à matriz de SIDs dos grupos de segurança do Active Directory em que o usuário está incluído. Por padrão, este campo no token de ID é chamado de 'groupsid'.

17. Clique no botão **Salvar**.

A integração com ADFS está concluída. Para entrar no Kaspersky Security Center Cloud Console com credenciais de conta AD, use o link fornecido na seção **Configurações de integração ADFS** (**Link de login para o Kaspersky Security Center Cloud Console com ADFS**).

Ao acessar o Kaspersky Security Center Cloud Console por meio do ADFS pela primeira vez, o console pode responder com um atraso.

Atribuir um usuário como um proprietário de dispositivo

Para obter informações sobre como atribuir um usuário como proprietário do dispositivo móvel, consulte a Ajuda do Kaspersky Security for Mobile.

Para atribuir um usuário como proprietário do dispositivo:

1. Caso queira atribuir um proprietário de um dispositivo conectado a um Servidor de Administração virtual, primeiro alterne para o Servidor de Administração virtual:
   a. No menu principal, clique no ícone de Sinalização ( ) à direita do nome atual do Servidor de Administração.
   b. Selecione o Servidor de Administração necessário.
2. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Usuários**.
   Uma lista de usuários é aberta. Caso você esteja conectado a um Servidor de Administração virtual, a lista incluirá usuários do Servidor de Administração virtual atual e do Servidor de Administração principal.
3. Clique no nome da conta de usuário que deseja atribuir como proprietário do dispositivo.
4. Na janela aberta de configurações do usuário, clique na guia **Dispositivos**.
5. Clique em **Adicionar**.
6. Na lista de dispositivos, selecione o dispositivo que deseja atribuir ao usuário.
7. Clique em **OK**.

O dispositivo selecionado é adicionado à lista de dispositivos atribuídos ao usuário.

Você pode executar a mesma operação em **Ativos (dispositivos)** → **Dispositivos gerenciados**, clicando no nome do dispositivo que deseja atribuir e clicando no link **Gerenciar proprietário do dispositivo**.

Gerenciar revisões de objeto

Esta seção contém informações sobre o gerenciamento de revisão de objeto.

Os objetos suportam o gerenciamento de revisão incluem:

- Servidores de Administração

- Políticas
- Tarefas
- Grupos de administração
- Contas de usuário
- Pacotes de instalação

Sobre as revisões do objeto

O Kaspersky Security Center Cloud Console permite rastrear as modificações em objetos. Cada vez quando você salva modificações feitas à um objeto, uma *revisão* é criada. Cada revisão tem um número.

Você pode executar as seguintes ações nas revisões do objeto:

- Exibir uma revisão selecionada
- Reverter as modificações feitas a um objeto para uma revisão selecionada

Na janela de propriedades de qualquer objeto que suporta o gerenciamento de revisão, a seção **Histórico de revisões** exibe uma lista de revisões de objeto com os seguintes detalhes:

- Número de revisão do objeto
- Data e hora em que o objeto foi modificado
- Nome do usuário que modificou o objeto
- A ação executada no objeto
- A descrição da revisão relativa à modificação feita nas configurações do objeto

  Por padrão, a descrição da revisão do objeto está em branco. Para adicionar uma descrição a uma revisão, selecione a revisão relevante e clique no botão **Editar descrição**. Na janela que se abre, digite um texto para a descrição da revisão.

Reverter modificações

Você poderá reverter as alterações feitas à um objeto, se necessário. Por exemplo, você poderá ter que reverter as configurações de uma política ao seu estado em uma data específica.

Para reverter as alterações feitas à um objeto:

1. Siga para a seção **Histórico de revisões** do objeto.
2. Na lista de revisões de objeto, selecione o número da revisão para a qual você precisa reverter as modificações.
3. Clique no botão **Reverter**.

O objeto é agora revertido à revisão selecionada. A lista de revisões de objeto exibe um registro da ação que foi executada. A descrição da revisão exibe as informações sobre o número da revisão à qual você reverteu o objeto.

Adicionar uma descrição da revisão

Você pode adicionar uma descrição da revisão para simplificar a procura por revisões na lista.

Para adicionar uma descrição para uma revisão:

1. Siga para a seção **Histórico de revisões** do objeto.
2. Na lista de revisões de objeto, selecione a revisão para a qual você precisa adicionar uma descrição.
3. Clique no botão **Editar descrição**.
4. Na janela que se abre, digite um texto para a descrição da revisão.
   Por padrão, a descrição da revisão do objeto está em branco.
5. Clique em **Salvar**.

A nova descrição é exibida na coluna **Descrição** da tabela do histórico de revisões.

Exclusão de objetos

Você pode excluir objetos, como os seguintes:

- Políticas
- Tarefas
- Pacotes de instalação
- Servidores de Administração virtual
- Usuários
- Grupos de segurança
- Grupos de administração

Quando você exclui um objeto, as informações sobre ele permanecem no banco de dados. O período de armazenamento das informações sobre os objetos excluídos é igual ao período de armazenamento das revisões de objetos (o período recomendado é de 90 dias). Você pode alterar o prazo de armazenamento somente se tiver a permissão **Modificar** na área de direitos **Objetos excluídos**.

Sobre a exclusão de dispositivos cliente

Quando um dispositivo gerenciado é excluído de um grupo de administração, o aplicativo move o dispositivo para o grupo dispositivos não atribuídos. Após a exclusão do dispositivo, os aplicativos Kaspersky instalados, o Agente de Rede e qualquer aplicativo de segurança, por exemplo, o Kaspersky Endpoint Security, permanecem no dispositivo.

O Kaspersky Security Center Cloud Console gerencia os dispositivos no grupo dispositivos não atribuídos de acordo com as seguintes regras:

- Caso tenha configurado as regras de movimentação de dispositivo e um dispositivo atenda aos critérios de uma regra de movimentação, o dispositivo é automaticamente movido para um grupo de administração de acordo com a regra.

- O dispositivo é armazenado no grupo dispositivos não atribuídos e é automaticamente removido do grupo de acordo com as regras de retenção de dispositivos.

  As regras de retenção de dispositivo não afetam os dispositivos que têm uma ou mais unidades criptografadas com criptografia completa do disco. Esses dispositivos não são excluídos automaticamente. Somente é possível excluí-los manualmente. Caso necessite excluir um dispositivo com uma unidade criptografada, primeiro descriptografe a unidade e, em seguida, exclua o dispositivo.

  Ao excluir um dispositivo com unidade criptografada, os dados necessários para descriptografar a unidade também são excluídos. Nesse caso, para descriptografar o dispositivo, as seguintes condições devem ser atendidas:

  - O dispositivo é reconectado ao Servidor de Administração para restaurar os dados necessários para descriptografar a unidade.

  - O usuário do dispositivo lembra a senha de descriptografia.

  - O aplicativo de segurança usado para criptografar o dispositivo, por exemplo, o Kaspersky Endpoint Security for Windows, ainda está instalado nele.

  Caso o dispositivo seja criptografado pela tecnologia Kaspersky Disk Encryption, também é possível tentar recuperar os dados usando o utilitário de restauração FDERT.

Quando um dispositivo é excluído manualmente do grupo dispositivos não atribuídos, o aplicativo remove o dispositivo da lista. Após a exclusão do dispositivo, os aplicativos Kaspersky instalados (se houver) permanecem no dispositivo. Em seguida, caso o dispositivo ainda esteja visível para o Servidor de Administração e o usuário tiver configurado a sondagem de rede regular, o Kaspersky Security Center Cloud Console descobre o dispositivo durante a sondagem de rede e o adiciona novamente ao grupo dispositivos não atribuídos. Portanto, é razoável excluir um dispositivo manualmente somente se o dispositivo estiver invisível para o Servidor de Administração.

Atualização dos bancos de dados e dos aplicativos da Kaspersky

Esta seção descreve as etapas que você deve seguir para atualizar regularmente o seguinte:

- Bancos de dados e módulos de software da Kaspersky
- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center Cloud Console

Cenário: Atualização regular dos bancos de dados e dos aplicativos da Kaspersky

Esta seção fornece um cenário para a atualização regular de bancos de dados, módulos de software e aplicativos da Kaspersky. Após concluir o cenário Configurando a proteção de rede, você deve manter a confiabilidade do sistema de proteção. Essa manutenção garante que a proteção dos dispositivos gerenciados permanece sólida contra uma variedade de ameaças, incluindo vírus, ataques à rede e ataques de phishing.

Há vários esquemas que você pode usar para instalar atualizações para componentes e aplicativos de segurança do Kaspersky Security Center Cloud Console. Selecione um ou mais esquemas ou vários esquemas que atendem aos requisitos de sua melhor rede.

O cenário abaixo descreve o esquema de atualização que implica o download de atualizações nos repositórios de pontos de distribuição. Caso os dispositivos gerenciados não tenham uma conexão aos pontos de distribuição, considere atualizar os bancos de dados, módulos do software e aplicativos da Kaspersky manualmente ou diretamente dos servidores de atualização da Kaspersky.

Ao concluir esse cenário, ocorrem os seguintes resultados:

- Os componentes do Kaspersky Security Center Cloud Console são atualizados automaticamente ou somente quando você designa o status *Aprovado* para as atualizações.
- Os aplicativos de segurança Kaspersky, os bancos de dados da Kaspersky e os módulos de software são atualizados de acordo com o agendamento que você especificou. Por padrão, os aplicativos de segurança Kaspersky instalam somente as atualizações que você aprova.

Você pode configurar o processo de atualização para baixar e instalar as atualizações de uma das duas maneiras a seguir:

- Automaticamente

  Nesse caso, você deve executar este cenário apenas uma vez. Você precisará agendar a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* (caso houver alguma), as tarefas de atualização para os aplicativos de segurança Kaspersky, além de manter as configurações de atualização padrão existentes nas propriedades do Agente de Rede.

- Manualmente

  Você pode configurar o processo de atualização para executar a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* (caso houver alguma) e as tarefas de atualização para os aplicativos de segurança Kaspersky manualmente. Você também pode configurar o Agente de Rede para instalar as atualizações dos componentes do Kaspersky Security Center Cloud Console apenas ao designar o status *Aprovado* para as atualizações.

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

1. Implementado os aplicativos de segurança Kaspersky nos dispositivos gerenciados de acordo com o cenário de implementação de aplicativos da Kaspersky através do Kaspersky Security Center Cloud Console. Ao executar o cenário, você atribuiu um volume apropriado de pontos de distribuição de acordo com o número de dispositivos gerenciados e com a topologia da rede.

2. Criado e configurado todos os perfis da política, políticas e tarefas necessários segundo o cenário de configuração da proteção de rede.

Fases

A configuração de atualizações regulares dos bancos de dados e dos aplicativos Kaspersky prossegue em fases:

1. **Criar a tarefa para baixar as atualizações aos repositórios de pontos de distribuição**

   Crie a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*. Quando esta tarefa for executada, o Kaspersky Security Center Cloud Console baixa as atualizações para os pontos de distribuição diretamente dos servidores de atualização da Kaspersky.

   Instruções de como proceder: Como criar a tarefa para baixar atualizações nos repositórios dos pontos de distribuição

2. **Configurar os pontos de distribuição**

   Certifique-se de que a opção **Implementar atualizações** esteja ativada nas propriedades de todos os pontos de distribuição necessários. Quando essa opção estiver desativada para um ponto de distribuição, os dispositivos incluídos no escopo do ponto de distribuição podem baixar as atualizações somente a partir de um recurso local ou diretamente dos servidores de atualização da Kaspersky.

   Se quiser que os dispositivos gerenciados recebam atualizações somente dos pontos de distribuição, ative a opção **Distribuir os arquivos somente através dos pontos de distribuição** na política de Agente de Rede.

3. **Otimização do processo usando arquivos diff (opcional)**

   Habilitar esse recurso resulta na redução no tráfego entre os pontos de distribuição e os dispositivos gerenciados. Para usar esse recurso, ative a opção **Baixar arquivos diff** nas propriedades da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*.

   Instruções de como proceder: Uso de arquivos diff para atualizar bancos de dados e módulos do software da Kaspersky

4. **Definindo quais atualizações instalar**

   Por padrão, as atualizações de software baixadas têm o status *Indefinido*. Altere o status para *Aprovado* ou *Negado* para definir se esta atualização deve ser instalada nos dispositivos em rede. As atualizações aprovadas sempre são instaladas. As atualizações não definidas só podem ser instaladas no Agente de Rede e em outros componentes do Kaspersky Security Center Cloud Console conforme as configurações de política do Agente de Rede. As atualizações para as quais você define o status *Negado* não serão instaladas em dispositivos.

   Instruções de como proceder:

   - Sobre o status de atualização
   - Aprovar e recusar atualizações de software

5. **Configurando a instalação automática de atualizações e patches para componentes do Kaspersky Security Center Cloud Console**

Por padrão, as atualizações e os patches baixados para o Agente de Rede e outros componentes do Kaspersky Security Center Cloud Console são instalados automaticamente. Se você deixou a opção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido** ativada nas propriedades do Agente de Rede, todas as atualizações serão instaladas automaticamente após o download no repositório (ou em vários repositórios). Se esta opção estiver desativada, as correções da Kaspersky que foram baixadas e identificadas com o status *Indefinido* somente serão instaladas após você alterar o status para *Aprovado*.

Instruções: Ativando e desativando a atualização automática e aplicando patches em componentes do Kaspersky Security Center Cloud Console

6. **Configuração da instalação automática de atualizações para os aplicativos de segurança**

   Crie a tarefa de Atualização para os aplicativos gerenciados para fornecer atualizações oportunas para os aplicativos, módulos do software e bancos de dados Kaspersky, inclusive bancos de dados de antivírus. Recomendamos selecionar a opção **Quando novas atualizações são baixadas no repositório** ao configurar o agendamento de tarefas. Isso garantirá que novas atualizações sejam instaladas o mais rápido possível.

   Por padrão, as atualizações para os aplicativos gerenciados são instaladas somente depois que você altera o status da atualização para *Aprovado*. No Kaspersky Endpoint Security for Windows, você pode alterar as configurações de atualização na tarefa Atualizar.

   Se uma atualização necessitar de análise e aceitação dos termos do Contrato de Licença do Usuário Final, você primeiro precisará aceitar os termos. Depois disso, a atualização poderá ser propagada para os dispositivos gerenciados.

   Instruções: A instalação automática do Kaspersky Endpoint Security efetua atualizações nos dispositivos

Após a conclusão do cenário, você poderá prosseguir com o monitoramento do status da rede.

Sobre atualização de bancos de dados, módulos de software e aplicativos da Kaspersky

Para ter certeza de que a proteção dos seus dispositivos gerenciados esteja atualizada, você deverá fornecer atualizações com frequência do seguinte:

- Bancos de dados e módulos de software da Kaspersky

  Antes de baixar os bancos de dados e módulos de software da Kaspersky, o Kaspersky Security Center Cloud Console verifica se os servidores da Kaspersky estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos. Isso é necessário para garantir que os bancos de dados antivírus sejam atualizados e que o nível de segurança seja mantido para os dispositivos gerenciados.

- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center Cloud Console

Dependendo da configuração da rede, você pode usar os seguintes esquemas de download e distribuição das atualizações necessárias para os dispositivos gerenciados:

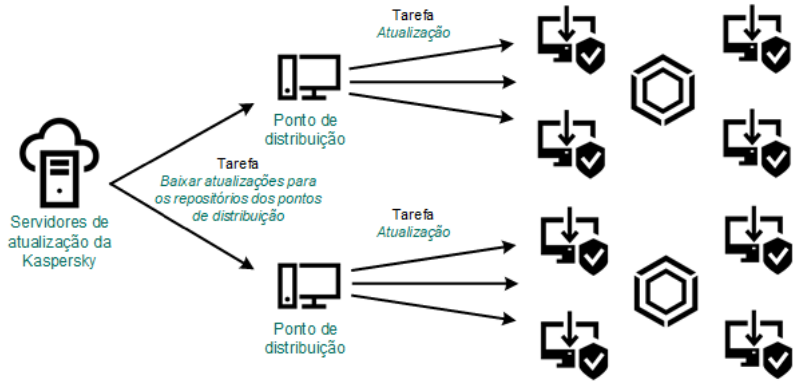
- Utilização da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*
- Manualmente por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP
- Diretamente dos servidores de atualização da Kaspersky para os aplicativos de segurança nos dispositivos gerenciados

Utilização da tarefa Baixar atualizações para os repositórios de pontos de distribuição

Nesse esquema, o Kaspersky Security Center Cloud Console baixa atualizações por meio da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*. Os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição (veja a figura abaixo).

Os dispositivos de ponto de distribuição executando macOS não podem baixar atualizações dos servidores de atualização da Kaspersky.

Se um ou mais dispositivos executando macOS estiverem dentro do escopo da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a tarefa será concluída com o status *Falha*, mesmo se for concluída com êxito em todos os dispositivos Windows.



Atualizando através da tarefa Baixar atualizações para os repositórios de pontos de distribuição

Quando a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for concluída, as seguintes atualizações serão baixadas no repositório do ponto de distribuição:

- Módulos de software e bancos de dados da Kaspersky para os aplicativos de segurança nos dispositivos gerenciados

  Essas atualizações são instaladas por meio da tarefa de Atualização para o Kaspersky Endpoint Security for Windows.

- Atualizações dos componentes do Kaspersky Security Center Cloud Console

  Por padrão, essas atualizações são instaladas automaticamente. Você pode alterar as configurações na política do Agente de rede.

- Atualizações dos aplicativos de segurança

  Por padrão, o Kaspersky Endpoint Security for Windows instala somente as atualizações que você aprova. As atualizações são instaladas por meio da tarefa de Atualização e podem ser configuradas nas propriedades desta tarefa.

Cada aplicativo da Kaspersky solicita as atualizações necessárias do Servidor de Administração. O Servidor de Administração agrega essas solicitações e baixa somente as atualizações que são solicitadas por qualquer aplicativo para os repositórios do ponto de distribuição. Isso garante que as mesmas atualizações não sejam baixadas várias vezes e impede que as atualizações desnecessárias sejam baixadas. Ao executar a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, o Servidor de Administração envia automaticamente as seguintes informações para os servidores de atualização da Kaspersky para assegurar o download das versões relevantes dos bancos de dados e dos módulos de software da Kaspersky:

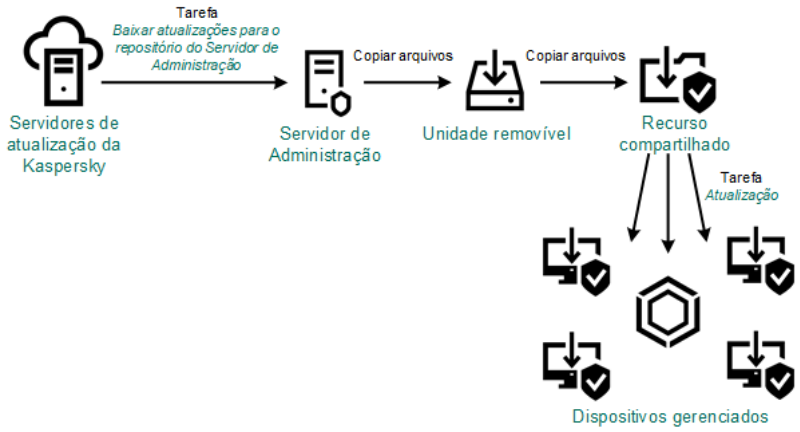
- ID e versão do aplicativo

- ID de instalação do aplicativo
- ID da chave ativa
- ID da execução da tarefa de download

Nenhuma das informações transmitidas contém informações pessoais ou outros dados confidenciais. A AO Kaspersky Lab protege as informações de acordo com os requisitos estabelecidos por lei.

Manualmente por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP

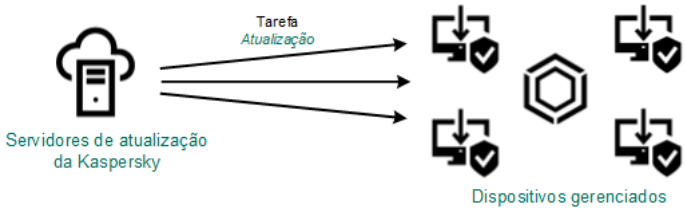
Se os dispositivos cliente não tiverem uma conexão com o ponto de distribuição, você poderá usar uma pasta local ou um recurso compartilhado como uma origem para atualizar os bancos de dados, módulos de software e aplicativos da Kaspersky. Nesse esquema, você tem que copiar as atualizações necessárias do repositório do ponto de distribuição para uma unidade removível e depois copiar as atualizações para a pasta local ou para o recurso compartilhado especificado como uma fonte de atualização nas configurações do Kaspersky Endpoint Security for Windows (veja a figura abaixo).



Atualização por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP

Diretamente dos servidores de atualização da Kaspersky para o Kaspersky Endpoint Security for Windows nos dispositivos gerenciados

Nos dispositivos gerenciados, você pode configurar o Kaspersky Endpoint Security for Windows para receber atualizações diretamente dos servidores de atualização da Kaspersky (veja a figura abaixo).



Atualização de aplicativos de segurança diretamente dos servidores de atualização da Kaspersky

Nesse esquema, o aplicativo de segurança não usa os repositórios fornecidos pelo Kaspersky Security Center Cloud Console. Para receber atualizações diretamente dos servidores de atualização da Kaspersky, especifique os servidores de atualização da Kaspersky como uma fonte de atualização na interface do aplicativo de segurança. Para uma descrição completa dessas configurações, consulte a documentação do Kaspersky Endpoint Security for Windows.

Criar a tarefa para baixar as atualizações aos repositórios de pontos de distribuição

Os dispositivos de ponto de distribuição executando macOS não podem baixar atualizações dos servidores de atualização da Kaspersky.

Se um ou mais dispositivos executando macOS estiverem dentro do escopo da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a tarefa será concluída com o status *Falha*, mesmo se for concluída com êxito em todos os dispositivos Windows.

Você pode criar a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* para um grupo de administração. Esta tarefa será executada para pontos de distribuição incluídos no grupo de administração especificado.

Esta tarefa é necessária para baixar atualizações de servidores de atualização da Kaspersky para os repositórios de pontos de distribuição. A lista de atualizações inclui:

- Atualizações para bancos de dados e módulos do software de aplicativos de segurança Kaspersky
- Atualizações para os componentes do Kaspersky Security Center Cloud Console
- Atualizações para aplicativos de segurança Kaspersky

Após o download das atualizações, elas podem ser propagadas aos dispositivos gerenciados.

Para criar a tarefa Baixar atualizações para os repositórios de pontos de distribuição para um grupo de administração selecionado:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique no botão **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center Cloud Console, no campo **Tipo de tarefa**, selecione **Baixar atualizações para os repositórios de pontos de distribuição**.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Selecione um botão de opção para especificar o grupo de administração, a seleção de dispositivos ou os dispositivos aos quais a tarefa se aplica.
6. Na opção **Concluir a criação da tarefa** etapa, se você ativar o **Abrir detalhes da tarefa quando a criação for concluída**, você pode modificar as configurações padrão da tarefa. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.
7. Clique no botão **Criar**.

   A tarefa é criada e exibida na lista de tarefas.
8. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

9. Na guia **Configurações do aplicativo** da janela de propriedades da tarefa, especifique as seguintes configurações:

- **Fontes de atualizações**

  Os seguintes recursos podem ser utilizados como uma origem das atualizações para o ponto de distribuição:

  - Servidores de atualização da Kaspersky

    Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.

    Esta opção está marcada por padrão.

  - Servidor de Administração Principal

    Este recurso é aplicado a tarefas criadas para um Servidor de Administração virtual ou secundário.

  - Pasta local ou de rede

    Uma pasta local ou pasta de rede que contém as atualizações mais recentes. Uma pasta de rede pode ser um servidor FTP ou HTTP, ou um compartilhamento SMB. Se uma pasta de rede exigir autenticação, apenas o protocolo SMB será compatível. Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado.

    Um servidor FTP ou HTTP ou pasta de rede utilizados por uma fonte de atualização devem conter uma estrutura de pastas (com atualizações) que corresponda à estrutura criada ao usar servidores de atualização Kaspersky.

- **Pasta para armazenar atualizações**

  O caminho para a pasta especificada para armazenar atualizações salvas. É possível copiar o caminho da pasta especificada para uma área de transferência. Não é possível alterar o caminho para uma pasta especificada para uma tarefa de grupo.

- **Baixar arquivos diff**

  Esta opção ativa o recurso de download dos arquivos diff.

  Por padrão, esta opção está desativada.

- **Baixar atualizações usando o esquema antigo**

O Kaspersky Security Center Cloud Console baixa atualizações de bancos de dados e módulos de software usando o novo esquema. Para que o aplicativo baixe atualizações usando o novo esquema, a fonte de atualização deve conter os arquivos de atualização com os metadados compatíveis com o novo esquema. Caso a fonte de atualização contenha os arquivos de atualização com os metadados compatíveis apenas com o esquema antigo, ative a opção **Baixar atualizações usando o esquema antigo**. Caso contrário, a tarefa de download de atualizações falhará.

Por exemplo, é preciso habilitar essa opção quando uma pasta local ou de rede for especificada como fonte de atualização, e os arquivos de atualização nesta pasta tiverem sido baixados por um dos seguintes aplicativos:

- Utilitário de atualização da Kaspersky

  Esse utilitário baixa as atualizações usando o esquema antigo.

- Kaspersky Security Center 13.2 ou versão anterior

Por exemplo, um ponto de distribuição está configurado para receber as atualizações de uma pasta local ou de rede. Nesse caso, é possível baixar as atualizações usando um Servidor de Administração que tenha uma conexão com a Internet e, em seguida, colocar as atualizações na pasta local no ponto de distribuição. Caso o Servidor de Administração tenha a versão 13.2 ou anterior, habilite a opção **Baixar atualizações usando o esquema antigo** na tarefa *Baixe atualizações para os repositórios de pontos de distribuição*.

Por padrão, esta opção está desativada.

10. Crie um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- Início agendado

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - Manualmente (selecionado por padrão)

    A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

    Por padrão, esta opção está ativada.

  - A cada N minutos

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - A cada N horas

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada seis horas, iniciando na data e hora atuais do sistema.

  - A cada N dias

A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

- **A cada N semanas**

  A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

  Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

- **Diariamente (não é compatível com horário de verão)**

  A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

  Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center Cloud Console.

  Por padrão, a tarefa inicia diariamente na hora atual do sistema.

- **Semanalmente**

  A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e na hora especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Todos os meses em dias especificados das semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

- **No surto de vírus**

A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

- Antivírus para estações de trabalho e servidores de arquivo
- Antivírus para defesa de perímetro
- Antivírus para sistemas de correio

Por padrão, todos os tipos de aplicativos estão selecionados.

Você pode precisar executar tarefas diferentes, dependendo do tipo de aplicativo antivírus que informa um ataque de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

  Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

  Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

  Se esta opção estiver desativada, somente as tarefas agendadas serão executadas nos dispositivos cliente; para **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas somente são executadas naqueles dispositivos cliente que estiverem visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

  Por padrão, esta opção está ativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos cliente aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos cliente aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

- **Usar atraso aleatório para inícios de tarefa em um intervalo de (min.)**

Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos cliente aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

11. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

    Além das configurações que você especificar durante a criação da tarefa, você pode alterar outras propriedades de uma tarefa criada.

Quando a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for executada, as atualizações para bancos de dados e módulos de software são baixadas da fonte de atualização e armazenadas na pasta compartilhada. As atualizações baixadas somente serão usadas por pontos de distribuição que estão incluídos no grupo de administração especificado e que não têm nenhuma tarefa de download de atualização explicitamente definida para eles.

Configurando dispositivos gerenciados para receber atualizações apenas de pontos de distribuição

Os dispositivos gerenciados podem recuperar atualizações dos bancos de dados Kaspersky, módulos de software e aplicativos Kaspersky de várias fontes: diretamente dos servidores de atualização, dos pontos de distribuição, ou de uma pasta local ou de rede. Você pode especificar pontos de distribuição como a única fonte possível de atualizações.

Para configurar os dispositivos gerenciados para receber atualizações apenas de pontos de distribuição:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique na política do Agente de Rede.
3. Na janela de propriedades da política, abra a guia **Configurações do aplicativo**.
4. Na seção **Configurações**, ative o botão **Distribuir os arquivos somente através dos pontos de distribuição**.
5. Defina o bloqueio (🔒) para este botão de alternância.
6. Clique no botão **Salvar**.

   A política será aplicada aos dispositivos selecionados e os dispositivos receberão atualizações apenas dos pontos de distribuição.

Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center Cloud Console

A instalação automática de atualizações e correções para componentes do Kaspersky Security Center Cloud Console é ativada por padrão durante a instalação do Agente de Rede no dispositivo. Você pode desativá-lo durante a instalação do Agente de Rede ou desativá-lo em outro momento usando uma política.

Para desativar a atualização automática e a correção para componentes do Kaspersky Security Center Cloud Console durante a instalação local do Agente de Rede em um dispositivo:

1. Inicie a instalação local do Agente de Rede no dispositivo.
2. Na etapa **Configurações avançadas**, desmarque a caixa de seleção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**.
3. Siga as instruções do Assistente.

   O Agente de Rede com a atualização e correção automática desativada para os componentes do Kaspersky Security Center Cloud Console será instalado no dispositivo. É possível ativar a atualização e a aplicação de patches automáticas mais tarde usando uma política.

Para desativar a atualização e a correção automática dos componentes do Kaspersky Security Center Cloud Console durante a instalação do Agente de Rede no dispositivo através de um pacote de instalação:

1. No menu principal, acesse **Operações → Repositórios → Pacotes de instalação**.
2. Clique no pacote **Agente de Rede do Kaspersky Security Center <número da versão>**.
3. Na janela Propriedades, selecione a guia **Configurações**.
4. Desligue o botão de alternância **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**.

   O Agente de Rede com a atualização e correção automática desativado para os componentes do Kaspersky Security Center Cloud Console será instalado a partir deste pacote. É possível ativar a atualização e a aplicação de patches automáticas mais tarde usando uma política.

Se a caixa de seleção na Etapa 4 foi selecionada (ou desmarcada) durante a instalação do Agente de Rede no dispositivo, você pode subsequentemente ativar (ou desativar) a atualização automática usando a política de Agente de Rede.

Para ativar ou desativar a atualização e a correção automática para os componentes do Kaspersky Security Center Cloud Console usando a política de Agente de Rede:

1. No menu principal, vá para **Ativos (dispositivos) → Políticas e perfis**.
2. Clique na política do Agente de Rede.
3. Na janela Propriedades da política, selecione a guia **Configurações do aplicativo**.
4. Na seção **Gerenciar patches e atualizações**, ative ou desative o botão de alternância **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido** para ativar ou desativar, respectivamente, a atualização e a aplicação de patches automáticas.

5. Certifique-se de definir (**Obrigar**) o bloqueio (🔒) para este botão de alternância.

A política será aplicada aos dispositivos selecionados, e a atualização e a correção automática para componentes do Kaspersky Security Center Cloud Console será ativada (ou desativada) nestes dispositivos.

Instalação automática de atualizações para o Kaspersky Endpoint Security for Windows

Você pode configurar as atualizações automáticas dos bancos de dados e módulos de software do Kaspersky Endpoint Security for Windows nos dispositivos cliente.

Para configurar o download e a instalação automática das atualizações do Kaspersky Endpoint Security for Windows nos dispositivos:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique no botão **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo da Kaspersky Endpoint Security for Windows, selecione **Atualização** como o subtipo de tarefa.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Selecione o escopo da tarefa.
6. Especifique o grupo de administração, a seleção de dispositivos ou os dispositivos aos quais a tarefa se aplica.
7. Na opção **Concluir a criação da tarefa** etapa, se você ativar o **Abrir detalhes da tarefa quando a criação for concluída**, você pode modificar as configurações padrão da tarefa. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.
8. Clique no botão **Criar**.

   A tarefa é criada e exibida na lista de tarefas.
9. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.
10. Na guia **Configurações do aplicativo** da janela de propriedades de tarefa, defina as configurações da tarefa de atualização no modo local ou de dispositivos móveis:

    - **Modo local**: as configurações nesta guia definem como o dispositivo recebe atualizações quando a conexão é estabelecida entre o dispositivo e o Servidor de Administração.
    - **Modo móvel**: as configurações nesta guia definem como o dispositivo recebe atualizações quando nenhuma conexão é estabelecida entre o Kaspersky Security Center Cloud Console e o dispositivo (por exemplo, quando o dispositivo não está conectado à Internet).
11. Ative as fontes de atualização que deseja usar para atualizar bancos de dados e módulos de aplicativo do Kaspersky Endpoint Security for Windows. Se necessário, altere as posições das fontes na lista usando os botões **Para cima** e **Para baixo**. Se várias fontes de atualizações forem ativadas, o Kaspersky Endpoint Security

for Windows tentará se conectar a elas uma após a outra, começando pelo topo da lista, e executará a tarefa de atualização recuperando o pacote de atualização da primeira fonte disponível.

Quando o Kaspersky Security Center Cloud Console estiver definido como uma fonte de atualização, as atualizações são baixadas de um repositório de ponto de distribuição e não do repositório do Servidor de Administração. Verifique se os pontos de distribuição foram atribuídos e se a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* foi criada.

12. Ative a opção **Instalar apenas atualizações aprovadas** para baixar e instalar atualizações dos módulos de software junto com bancos de dados do aplicativo.

    Se a opção estiver ativada, o Kaspersky Endpoint Security for Windows notifica o usuário sobre as atualizações dos módulos de software disponíveis e inclui atualizações nos módulos de software no pacote de atualização ao executar a tarefa de atualização. O Kaspersky Endpoint Security for Windows instala somente as atualizações para as quais você definiu o status *Aprovado*; elas serão instaladas localmente por meio da interface do aplicativo ou do Kaspersky Security Center Cloud Console.

    Você também pode ativar a opção **Instalar atualizações críticas do módulo de aplicativo automaticamente**. Se quaisquer atualizações do módulo de software estiverem disponíveis, o Kaspersky Endpoint Security for Windows as instala com o status *Crítico*; as atualizações remanescentes serão instaladas após a sua aprovação.

    Se a atualização do módulo de software requerer a revisão e aceitação dos termos do Contrato de Licença e da Política de Privacidade, o aplicativo instala as atualizações após os termos do Contrato de Licença e da Política de Privacidade terem sido aceitos pelo usuário.

13. Marque a caixa de seleção **Copiar atualizações para uma pasta** para que o aplicativo salve as atualizações baixadas em uma pasta e especifique o caminho da pasta.

14. Agende a tarefa. Para assegurar atualizações oportunas, recomendamos selecionar a opção **Quando novas atualizações são baixadas no repositório**.

15. Clique em **Salvar**.

Ao executar a tarefa de **Atualização**, o aplicativo envia solicitações aos servidores de atualização Kaspersky.

Algumas atualizações necessitam da instalação das versões mais recentes dos plug-ins de gerenciamento.

Sobre o status de atualização

Status é um atributo das atualizações de software que define se uma atualização de software particular deve ser instalada em um dispositivo em rede.

Uma atualização pode ter os seguintes status:

- *Indefinido*

  Por padrão, as atualizações de software baixadas têm o status *Indefinido*. As atualizações não definidas só podem ser instaladas no Agente de Rede e em outros componentes do Kaspersky Security Center Cloud Console conforme as configurações de política do Agente de Rede.

- *Aprovado*

  As atualizações aprovadas sempre são instaladas. Se uma atualização necessitar de análise e aceitação dos termos do Contrato de Licença do Usuário Final, você primeiro precisará aceitar os termos.

- *Negado*

  As atualizações para as quais você define o status *Negado* não serão instaladas em dispositivos.

Você pode alterar os status das atualizações para o seguinte software:

- Agente de Rede e outros componentes do Kaspersky Security Center Cloud Console

  Por padrão, as atualizações e os patches baixados para o Agente de Rede e outros componentes do Kaspersky Security Center Cloud Console são instalados automaticamente. Se você deixou a opção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido** ativada nas propriedades do Agente de Rede, todas as atualizações serão instaladas automaticamente após o download no repositório (ou em vários repositórios). Se esta opção estiver desativada, as correções da Kaspersky que foram baixadas e identificadas com o status *Indefinido* somente serão instaladas após você alterar o status para *Aprovado*.

  As atualizações dos componentes do Kaspersky Security Center Cloud Console não podem ser desinstaladas, mesmo se você definir o status *Negado*.

- Aplicativos de segurança Kaspersky

  Por padrão, as atualizações para os aplicativos gerenciados são instaladas somente depois que você altera o status da atualização para *Aprovado*. Se uma atualização recusada para um aplicativo de segurança tiver sido instalada anteriormente, o Kaspersky Security Center Cloud Console tentará desinstalar a atualização de todos os dispositivos.

Aprovar e recusar atualizações de software

As configurações de uma tarefa de instalação de atualização podem necessitar da aprovação de atualizações que devem ser instaladas. Você pode aprovar atualizações que devem ser instaladas e recusar as atualizações que não devem ser instaladas.

Por exemplo, pode ser necessário verificar primeiro a instalação das atualizações em um ambiente de teste, assegurar-se de que elas não interferem na operação dos dispositivos e, só então, permitir a instalação dessas atualizações nos dispositivos cliente.

Para aprovar ou recusar uma ou várias atualizações:

1. No menu principal, vá para **Operações → Aplicativos Kaspersky → Atualizações contínuas**.

   Aparece uma lista das atualizações disponíveis.

   > As atualizações de aplicativos gerenciados podem exigir a instalação de uma versão mínima específica do Kaspersky Security Center. Se esta versão for posterior à versão atual, essas atualizações serão exibidas, mas não poderão ser aprovadas. Além disso, nenhum pacote de instalação pode ser criado a partir dessas atualizações até que você atualize o Kaspersky Security Center. Você receberá uma solicitação para atualizar sua instância do Kaspersky Security Center para a versão mínima necessária.

2. Selecione as atualizações que deseja aprovar ou recusar.

3. Clique em **Aprovar** para aprovar as atualizações selecionadas ou **Recusar** para recusar as atualizações selecionadas.

O valor padrão é *Indefinido*.

As atualizações às quais você atribui o status *Aprovado* são colocadas em uma fila para instalação.

As atualizações às quais você atribui o status *Negado* são desinstaladas (se possível) de todos os dispositivos nos quais elas foram anteriormente instaladas. Além disso, elas não serão instaladas em outros dispositivos no futuro.

Algumas atualizações para aplicativos da Kaspersky não podem ser desinstaladas. Se você definir o status *Recusado*, o Kaspersky Security Center Cloud Console não desinstalará estas atualizações dos dispositivos nos quais estão instaladas. No entanto, essas atualizações nunca serão instaladas em outros dispositivos no futuro.

Se você definir o status *Negado* para atualizações de software de terceiros, estas atualizações não serão instaladas em dispositivos para os quais elas foram planejadas, mas que ainda não foram instaladas. As atualizações permanecerão nos dispositivos nos quais elas já foram instaladas. Se você tiver as atualizações, poderá exclui-las de forma manual localmente.

Uso de arquivos diff para atualizar bancos de dados e módulos do software da Kaspersky

Um arquivo diff descreve as diferenças entre duas versões de um arquivo de banco de dados ou módulo de software. O uso de arquivos diff limita o tráfego na rede da empresa porque os arquivos diff ocupam menos espaço do que arquivos completos de bancos de dados e módulos de software. Se o recurso *Baixar arquivos diff* estiver ativado em um ponto de distribuição, os arquivos diff serão salvos neste ponto de distribuição. Como resultado, os dispositivos que recebem atualizações desse ponto de distribuição podem usar os arquivos diff salvos para atualizar bancos de dados e módulos de software.

Para otimizar o uso de arquivos diff, recomendamos que você sincronize os agendamentos das atualizações dos dispositivos com os do ponto de distribuição a partir do qual os dispositivos são atualizados. Entretanto, pode ocorrer economia de tráfego mesmo se os dispositivos forem atualizados com muito menos frequência do que o ponto de distribuição a partir do qual os dispositivos são atualizados.

Os pontos de distribuição não usam multicasting de IP para distribuição automática de arquivos diff.

Para ativar o recurso Baixar arquivos diff:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique na tarefa *Baixar atualizações para os repositórios de pontos de distribuição* para abrir suas propriedades.
3. Na guia **Configurações do aplicativo**, ative a opção **Baixar arquivos diff**.
4. Clique no botão **Salvar**.

O recurso Download de arquivos diff está ativado. Arquivos Diff de atualizações serão baixados, além dos arquivos de atualização, sempre que a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for executada.

Para verificar se o recurso Baixar arquivos diff está ativado com êxito, você pode medir o tráfego interno antes e depois de executar o cenário.

Atualização de bancos de dados e módulos de software da Kaspersky em dispositivos offline

A atualização dos bancos de dados e dos módulos de software da Kaspersky em dispositivos gerenciados é uma tarefa importante para manter a proteção dos dispositivos contra vírus e outras ameaças. Os administradores normalmente configuram atualizações regulares através do uso do repositório dos repositórios de pontos de distribuição.

Quando for preciso atualizar os bancos de dados e módulos do software em um dispositivo (ou um grupo de dispositivos) que não está conectado ao ponto de distribuição ou à Internet, você terá de usar fontes alternativas de atualizações, tal como um servidor FTP ou uma pasta local. Nesse caso, você precisa entregar os arquivos das atualizações necessárias usando um dispositivo de armazenamento em massa, como um pen drive ou um disco rígido externo.

Você pode copiar as atualizações necessárias das seguintes fontes:

- Ponto de distribuição.

  Para ter certeza de que o repositório do ponto de distribuição contém as atualizações necessárias para o aplicativo de segurança instalado em um dispositivo offline, pelo menos um dos dispositivos online gerenciados do ponto de distribuição deve ter o mesmo aplicativo de segurança instalado. Este aplicativo deve ser configurado para receber as atualizações do repositório do ponto de distribuição por meio da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*.

- Qualquer dispositivo que tenha o mesmo aplicativo de segurança instalado e configurado para receber as atualizações de um repositório de ponto de distribuição ou diretamente dos servidores de atualização da Kaspersky.

Abaixo há um exemplo de configuração de atualizações de bancos de dados e módulos de software copiando-os do repositório do ponto de distribuição.

Para atualizar os bancos de dados e módulos de software da Kaspersky em dispositivos offline:

1. Conecte a unidade removível ao dispositivo do ponto de distribuição.

2. Copie os arquivos de atualizações para a unidade removível.

   Por padrão, as atualizações estão localizadas em: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates.

3. Em dispositivos offline, configure o aplicativo de segurança (por exemplo, Kaspersky Endpoint Security for Windows) para receber atualizações de uma pasta local ou um recurso compartilhado, como um Servidor FTP ou uma pasta compartilhada.

4. Copie os arquivos de atualizações da unidade removível para a pasta local ou o recurso compartilhado que deseja usar como uma fonte de atualização.

5. No dispositivo offline que requer a instalação de atualização, inicie a tarefa de atualização do Kaspersky Endpoint Security for Windows.

Depois que a tarefa de atualização for concluída, os bancos de dados e os módulos de software da Kaspersky serão atualizados no dispositivo.

Atualização do Kaspersky Security for Windows Server

É possível instalar o Kaspersky Security for Windows Server em dispositivos gerenciados; pode ser que você queira iniciar a tarefa de Proteção do arquivo em tempo real desse aplicativo. No entanto, o aplicativo é fornecido sem os bancos de dados necessários para o funcionamento correto. Os bancos de dados são baixados para o dispositivo gerenciado somente depois que a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for concluída.

Caso deseje iniciar a tarefa de Proteção de arquivo em tempo real em um dispositivo gerenciado logo após a instalação do Kaspersky Security for Windows Server, certifique-se de que os bancos de dados do aplicativo foram baixados e estão atualizados. Caso contrário, a tarefa pode funcionar incorretamente.

Para garantir que os bancos de dados do Kaspersky Security for Windows Server estão atualizados:

1. Certifique-se de que a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* foi concluída no Servidor de Administração.

2. Execute uma das seguintes ações:

   - Nas configurações da tarefa de Proteção de arquivo em tempo real, defina o início como *Na inicialização do aplicativo* e reinicie o dispositivo gerenciado.

   - Nas configurações da tarefa de Proteção de arquivo em tempo real, defina manualmente a hora de início para a hora desejada.

A tarefa de Proteção de arquivo em tempo real no Kaspersky Security for Windows Server está pronta para funcionar corretamente.

Gerenciar aplicativos de terceiros em dispositivos cliente

Esta seção descreve os recursos do Kaspersky Security Center Cloud Console relacionados ao gerenciamento de aplicativos de terceiros instalados nos dispositivos cliente.

Sobre aplicativos de terceiros

O Kaspersky Security Center Cloud Console pode ajudar a atualizar softwares de terceiros instalados em dispositivos clientes e também a corrigir as vulnerabilidades. O Kaspersky Security Center Cloud Console pode atualizar softwares de terceiros apenas da versão atual para a versão mais recente. A lista a seguir apresenta os softwares de terceiros que você pode atualizar com o Kaspersky Security Center:

A lista de softwares de terceiros pode ser atualizada e ampliada com novos aplicativos. Confira se é possível atualizar o software de terceiros (instalado nos dispositivos dos usuários) com o Kaspersky Security Center Cloud Console ao consultando a lista de atualizações disponíveis no Kaspersky Security Center Cloud Console.

- 7-Zip Developers: 7-Zip
- Adobe Systems:
  - Adobe Acrobat DC
  - Adobe Acrobat Reader DC
  - Adobe Acrobat
  - Adobe Reader
  - Adobe Shockwave Player
- AIMPDevTeam: AIMP
- ALTAP: Altap Salamander
- Apache Software Foundation: Apache Tomcat
- Apple:
  - Apple iTunes
  - Apple QuickTime
- Armory Technologies, Inc.: Armory
- Cerulean Studios: Trillian Basic
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber
- Code Sector: TeraCopy

- Codec Guide:
  - K-Lite Codec Pack Basic
  - K-Lite Codec Pack Full
  - K-Lite Codec Pack Mega
  - K-Lite Codec Pack Standard
- DbVis Software AB: DbVisualizer
- Decho Corp.:
  - Mozy Enterprise
  - Mozy Home
  - Mozy Pro
- Dominik Reichl: KeePass Password Safe
- Don HO don.h@free.fr: Notepad++
- DoubleGIS: 2GIS
- Dropbox, Inc.: Dropbox
- EaseUs: EaseUS Todo Backup Free
- Electrum Technologies GmbH: Electrum
- Enter Srl: Iperius Backup
- Eric Lawrence: Fiddler
- EverNote: EverNote
- Exodus Movement Inc: Exodus
- EZB Systems: UltraISO
- Famatech:
  - Radmin
  - Remote Administrator
- Far Manager: FAR Manager
- FastStone Soft: FastStone Image Viewer
- FileZilla Project: FileZilla
- Firebird Developers: Firebird

- Foxit Corporation:
  - Foxit Reader
  - Foxit Reader Enterprise
- Free Download Manager.ORG: Free Download Manager
- GIMP project: GIMP
- GlavSoft LLC.: TightVNC
- GNU Project: Gpg4win
- Google:
  - Google Earth
  - Google Chrome
  - Google Chrome Enterprise
  - Google Earth Pro
- Inkscape Project: Inkscape
- IrfanView: IrfanView
- iterate GmbH: Cyberduck
- Logitech: SetPoint
- LogMeIn, Inc.:
  - LogMeIn
  - Hamachi
  - LogMeIn Rescue Technician Console
- Martin Prikryl: WinSCP
- Mozilla Foundation:
  - Mozilla Firefox
  - Mozilla Firefox ESR
  - Mozilla SeaMonkey
  - Mozilla Thunderbird
- New Cloud Technologies Ltd: MyOffice Standard. Home Edition
- OpenOffice.org: OpenOffice

- Opera Software: Opera
- Oracle Corporation:
  - Oracle Java JRE
  - Oracle VirtualBox
- PDF44: PDF24 MSI/EXE
- Piriform:
  - CCleaner
  - Defraggler
  - Recuva
  - Speccy
- Postgresql: PostgreSQL
- RealNetworks: RealPlayer Cloud
- RealVNC:
  - RealVNC Server
  - RealVNC Viewer
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (completo/mínimo)
- Simon Tatham: PuTTY
- Skype Technologies: Skype para Windows
- Sober Lemur S.a.s:
  - PDFsam Basic
  - PDFsam Visual
- Softland: FBackup
- Splashtop Inc.: Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP
- Sublime HQ Pty Ltd: Sublime Text
- TeamViewer GmbH:
  - TeamViewer Host
  - TeamViewer

- Telegram Messenger LLP: Telegram Desktop
- The Document Foundation:
  - LibreOffice
  - LibreOffice HelpPack
- The Git Development Community:
  - Git for Windows
  - Git LFS
- The Pidgin developer community: Pidgin
- TortoiseSVN Developers: TortoiseSVN
- VideoLAN: VLC media player
- VMware:
  - VMware Player
  - VMware Workstation
- WinRAR Developers: WinRAR
- WinZip: WinZip
- Wireshark Foundation: Wireshark
- Wrike: Wrike
- Zimbra: Zimbra Desktop

Limitações do Gerenciamento de patches e vulnerabilidades

O recurso Gerenciamento de patches e vulnerabilidades possui uma série de limitações, dependendo da licença utilizada e do modo em que o Kaspersky Security Center Cloud Console está funcionando.

As seguintes licenças não oferecem suporte ao recurso de Gerenciamento de patches e vulnerabilidades:

- Kaspersky Endpoint Security for Business Select
- Kaspersky Hybrid Cloud Security

As seguintes licenças oferecem o recurso de Gerenciamento de patches e vulnerabilidades:

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Detection and Response Optimum

- Kaspersky Total Security for Business
- Kaspersky Hybrid Cloud Security Enterprise

A tabela abaixo compara as limitações do Kaspersky Security Center Cloud Console em modo de avaliação, com licenças que oferecem e que não oferecem suporte ao recurso de Gerenciamento de patches e vulnerabilidades.

Limitações do Gerenciamento de patches e vulnerabilidades

Limitação	Modo de avaliação	Modo comercial: licenças que não oferecem suporte ao recurso de Gerenciamento de patches e vulnerabilidades	Modo comercial: licenças que oferecem o recurso de gerenciamento de patches e vulnerabilidades
Número máximo de tarefas *Instalar as atualizações do Windows Update* ou de tarefas *Corrigir vulnerabilidades*	4	4	0 (novas tarefas desses tipos não podem ser criadas)
Número máximo de tarefas *Instalar as atualizações necessárias e corrigir vulnerabilidades*	2	Sem suporte	4
Número máximo de regras em todas as tarefas *Instalar as atualizações necessárias e corrigir vulnerabilidades*	10	Sem suporte	50
Número máximo de atualizações de software que podem ter o status *Aprovado* ao mesmo tempo	100	Sem suporte	1000
Número máximo de atualizações de software que podem ser adicionadas manualmente a uma tarefa	500	1000	1000
Número máximo de vulnerabilidades de software que podem ser adicionadas manualmente a uma tarefa	500	1000	1000

Disponibilidade de recursos de Gerenciamento de patches e vulnerabilidades em modo de teste e comercial e sob várias opções de licenciamento

A disponibilidade dos recursos de Gerenciamento de patches e vulnerabilidades no Kaspersky Security Center Cloud Console depende se você está usando o modo de teste ou comercial, bem como da opção de licenciamento selecionada. Use a tabela para verificar quais recursos de Gerenciamento de patches e vulnerabilidades estão disponíveis.

Disponibilidade dos recursos de Gerenciamento de patches e vulnerabilidades

O recurso Gerenciamento	Modo de avaliação	Modo comercial - Kaspersky Endpoint Security for Business Select	Modo co Kaspersky Endpoint Securi

de patches e vulnerabilidades			Kaspersky Endpoint Detecti Kaspersky Total Se
Correção manual de vulnerabilidades em softwares Microsoft em dispositivos gerenciados que executam o Windows Criar a tarefa *Corrigir vulnerabilidades*	✓	✓	–
Instalação manual de atualizações em softwares Microsoft em dispositivos gerenciados com sistema operacional Windows Instalação das atualizações de software de terceiros por meio da tarefa *Instalar as atualizações do Windows Update*	–	✓	✓
Instalação automática baseada em regras de atualizações de softwares de terceiros e correção de vulnerabilidades de softwares de terceiros Criação da tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* e instalação de atualizações Adicionar regras para instalação da atualização	✓	–	✓

Instalar atualizações de software de terceiros

Esta seção descreve os recursos do Kaspersky Security Center Cloud Console relacionados à instalação de atualizações para aplicativos de terceiros instalados nos dispositivos cliente.

Cenário: Atualizando software de terceiros

Esta seção fornece um cenário para a atualização software de terceiros instalados nos dispositivos cliente. Software de terceiros incluem aplicativos da Microsoft e de outros fornecedores de software. As atualizações para aplicativos Microsoft são fornecidas pelo serviço Windows Update.

Fases

A atualização de software de terceiros prossegue em fases:

1. **Procurar atualizações necessárias**

   Para encontrar as atualizações de softwares de terceiros necessárias para os dispositivos gerenciados, execute a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Kaspersky Security Center Cloud Console recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa.

   A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente pelo Assistente de Início Rápido do Servidor de Administração. Caso não tenha executado o assistente, crie a tarefa ou execute o Assistente de Início Rápido rápido agora.

   Instruções de como proceder:

   - Criar uma tarefa Encontrar as vulnerabilidades e as atualizações necessárias
   - As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias

2. **Analisar a lista de atualizações encontradas**

   Exiba a lista **Atualizações de software** e decida quais atualizações devem ser instaladas. Para visualizar informações detalhadas sobre cada atualização, clique no nome da atualização na lista. Para cada atualização na lista, você pode visualizar as estatísticas sobre a instalação da atualização nos dispositivos gerenciados. Por exemplo, você pode visualizar o número de dispositivos nos quais a atualização selecionada não está instalada, será instalada ou no qual a atualização falhou.

   Instruções de como proceder: Visualizar informações sobre atualizações de software de terceiros disponíveis

3. **Configurar instalação de atualizações**

   Quando o Kaspersky Security Center Cloud Console tiver recebido a lista de atualizações de softwares de terceiros, será possível instalá-las em dispositivos cliente usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. Crie uma dessas tarefas. Você pode criar essas tarefas na guia **Tarefas** ou usando a lista **Atualizações de software**.

   A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para instalar atualizações para aplicativos da Microsoft, incluindo as atualizações fornecidas pelo serviço Windows Update e as atualizações de produtos de outros fornecedores.

   A tarefa *Instalar as atualizações do Windows Update* é usada para instalar apenas atualizações do Windows Update.

As tarefas de instalação da atualização de software têm uma série de limitações. Essas limitações dependem da licença sob a qual você está usando o Kaspersky Security Center Cloud Console e do modo em que o Kaspersky Security Center Cloud Console está operando.

Para instalar algumas atualizações de software, você deve aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software. Se você recusar o EULA, a atualização do software não será instalada.

Instruções de como proceder:

- Criar a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades
- Criar a tarefa Instalar as atualizações do Windows Update
- Exibir informações sobre atualizações disponíveis para software de terceiros

4. **Agendar as tarefas**

   Para garantir que a lista de atualizações esteja sempre atualizada, agende a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para executá-la automaticamente de tempos em tempos. A frequência padrão é de uma vez por semana.

   Se você criou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, pode agendá-la para ser executada com a mesma frequência que a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou com menor frequência. Ao agendar a tarefa *Instalar as atualizações do Windows Update*, observe que, para essa tarefa, é necessário definir a lista de atualizações todas as vezes antes de iniciá-la.

   Ao agendar as tarefas, certifique-se que uma tarefa para corrigir vulnerabilidades é iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

   Instruções de uso: Configurações gerais da tarefa

5. **Aprovar e recusar atualizações de software (opcional)**

   Caso você tenha criado a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, será possível especificar regras para instalação da atualização nas propriedades da tarefa. Caso tenha criado a tarefa *Instalar as atualizações do Windows Update*, pule esta etapa.

   Para cada regra, você pode definir as atualizações a serem instaladas, dependendo do status da atualização: *Indefinido*, *Aprovado* ou *Recusado*. Por exemplo, convém criar uma tarefa específica para servidores e definir uma regra para essa tarefa para permitir a instalação apenas de atualizações do Windows Update e somente aquelas com status *Aprovado*. Depois disso, você define manualmente o status *Aprovado* para as atualizações que deseja instalar. Nesse caso, as atualizações do Windows Update com status *Indefinido* ou *Recusado* não serão instaladas nos servidores especificados para a tarefa.

   Por padrão, as atualizações de software baixadas têm o status *Indefinido*. Você pode alterar o status para *Aprovado* ou *Recusado* na lista **Atualizações de software** (**Operações → Gerenciamento de patches → Atualizações de software**).

   Instruções sobre como proceder: Aprovar e recusar as atualizações de softwares de terceiros

6. **Executar uma tarefa de instalação de atualização**

   Inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. Quando você inicia essas tarefas, as atualizações são baixadas e instaladas nos dispositivos gerenciados. Após a conclusão da tarefa, verifique se ela possui o status *Concluída com êxito* na lista de tarefas.

   Instruções de uso: Iniciando uma tarefa manualmente

7. **Criar o relatório sobre os resultados da instalação da atualização de software de terceiros (opcional)**

   Para garantir que a tarefa seja criada e as atualizações instaladas, crie o **Relatório de resultados da instalação de atualizações de software de terceiros** e visualize as estatísticas detalhadas sobre a instalação da atualização neste relatório.

   Instruções de como proceder: Gerar e visualizar um relatório

Sobre as atualizações de software de terceiros

O Kaspersky Security Center Cloud Console permite gerenciar as atualizações do software de terceiros instalado em dispositivos gerenciados e corrigir vulnerabilidade em aplicativos Microsoft e de produtos de outros fornecedores através da instalação das atualizações necessárias.

O Kaspersky Security Center Cloud Console procura atualizações por meio da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Servidor de Administração recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa. Após visualizar as informações sobre as atualizações disponíveis, você pode instalar as mesmas nos dispositivos.

O Kaspersky Security Center Cloud Console atualiza alguns aplicativos ao remover a versão anterior e instalar a nova versão.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Por motivos de segurança, todas as atualizações de software de terceiros que você instala usando o recurso Gerenciamento de Patches e Vulnerabilidades são verificadas automaticamente em busca de malwares pelas tecnologias da Kaspersky. Essas tecnologias são usadas para verificação automática de arquivos e incluem verificação de vírus, análise estática, análise dinâmica, análise de comportamento no ambiente sandbox e aprendizado de máquina.

Os especialistas da Kaspersky não realizam análises manuais de atualizações de softwares de terceiros que podem ser instaladas usando o recurso Gerenciamento de patches e vulnerabilidades. Além disso, os especialistas da Kaspersky não pesquisam vulnerabilidades (conhecidas ou desconhecidas) ou recursos não documentados nessas atualizações, nem realizam outros tipos de análise das atualizações além dos especificados no parágrafo acima.

Tarefas para instalação das atualizações de software de terceiros

Quando os metadados das atualizações de software de terceiros são baixados para o repositório, você pode instalar as atualizações nos dispositivos clientes usando as seguintes tarefas:

- A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*

  Esta tarefa é usada para instalar atualizações para aplicativos Microsoft, incluindo as atualizações fornecidas pelo serviço Windows Update e as atualizações de produtos de outros fornecedores.

  Quando essa tarefa é concluída, as atualizações são instaladas nos dispositivos gerenciados automaticamente. Quando os metadados das novas atualizações são baixados no repositório do Servidor de Administração, o Kaspersky Security Center Cloud Console verifica se as atualizações atendem aos critérios especificados nas regras de atualização. Todas as novas atualizações que atendem aos critérios serão baixadas e instaladas automaticamente na próxima tarefa executada.

- A tarefa *Instalar as atualizações do Windows Update*

  Esta tarefa é usada para instalar apenas atualizações do Windows Update.

  Quando esta tarefa é concluída, apenas as atualizações especificadas nas propriedades da tarefa são instaladas. No futuro, caso deseje instalar novas atualizações, você deve adicionar as atualizações necessárias à lista de atualizações da tarefa existente ou criar uma tarefa *Instalar as atualizações do Windows Update*.

As tarefas de instalação da atualização de software têm uma série de limitações. Essas limitações dependem da licença sob a qual você está usando o Kaspersky Security Center Cloud Console e do modo em que o Kaspersky Security Center Cloud Console está operando.

Instalar atualizações de software de terceiros

É possível instalar atualizações de softwares de terceiros em dispositivos gerenciados criando e executando uma das seguintes tarefas:

- *Instalar as atualizações necessárias e corrigir vulnerabilidades*

  Você pode usar esta tarefa para instalar as atualizações do Windows Update fornecidas pela Microsoft e atualizações de produtos de outros fornecedores.

- *Instalar as atualizações do Windows Update*

  Você pode usar essa tarefa para instalar apenas atualizações do Windows Update.

As tarefas de instalação da atualização de software têm uma série de limitações. Essas limitações dependem da licença sob a qual você está usando o Kaspersky Security Center Cloud Console e do modo em que o Kaspersky Security Center Cloud Console está operando.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Como opção, é possível criar uma tarefa para instalar as atualizações necessárias das seguintes maneiras:

- Abrindo a lista de atualizações e especificando quais atualizações instalar.

  Como resultado, é criada uma nova tarefa para instalar as atualizações selecionadas. Como opção, você pode adicionar as atualizações selecionadas a uma tarefa existente.

- Executando o assistente de Instalação de atualizações.

  A disponibilidade do assistente de instalação de atualizações depende do modo do Kaspersky Security Center Cloud Console e da licença atual.

  O assistente simplifica a criação e configuração de uma tarefa de instalação de atualizações e permite eliminar a criação de tarefas redundantes que contenham as mesmas atualizações a serem instaladas.

Instalar atualizações de softwares de terceiros usando a lista de atualizações

Para instalar atualizações de software de terceiros usando a lista de atualizações:

1. Abra uma das listas de atualizações:

   - Para abrir a lista geral de atualização, No menu principal, vá para **Operações → Gerenciamento de patches → Atualizações de software**.

- Para abrir a lista de atualizações de um dispositivo gerenciado, no meu principal, acesse **Ativos (dispositivos)** → **Dispositivos gerenciados** → **<dispositivo gerenciado>** → **Avançado** → **Atualizações disponíveis**.

- Para abrir a lista de atualizações de um aplicativo específico, no meu principal, acesse **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos** → **<nome do aplicativo>** → **Atualizações disponíveis**.

Aparece uma lista das atualizações disponíveis.

2. Marque as caixas de seleção ao lado das atualizações que deseja baixar.

3. Clique no botão **Instalar as atualizações**.

   Para instalar algumas atualizações de software, você deve aceitar o Contrato de Licença do Usuário Final (EULA). Se você recusar o EULA, a atualização do software não será instalada.

4. Selecione uma das seguintes opções:

   - **Nova tarefa**

     O Assistente para nova tarefa inicia. A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update* é pré-selecionada, dependendo do Kaspersky Security Center Cloud Console e de sua licença atual. Seguem abaixo as etapas do assistente para concluir a criação da tarefa.

   - **Instalar a atualização (adicionar a regra à tarefa especificada)**

     Selecione uma tarefa à qual deseja adicionar as atualizações selecionadas. Selecione a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. Se você selecionar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, uma nova regra para instalar as atualizações selecionadas será adicionada automaticamente à tarefa escolhida. Se você selecionar a tarefa *Instalar as atualizações do Windows Update*, as atualizações selecionadas serão adicionadas às propriedades da tarefa.

     A janela de propriedades da tarefa é aberta. Clique no botão **Salvar** para salvar as alterações.

Se você escolheu criar uma nova tarefa, a tarefa será criada e exibida na lista de tarefas em **Ativos (dispositivos)** → **Tarefas**. Se você optou por adicionar as atualizações a uma tarefa existente, as atualizações serão salvas nas propriedades da tarefa.

Para instalar atualizações de software de terceiros, inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. É possível iniciar qualquer uma dessas tarefas manualmente ou especificar configurações de agendamento nas propriedades da tarefa iniciada. Ao especificar o agendamento de tarefas, certifique-se de que a tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

Instalar atualizações de softwares de terceiros usando o assistente de Instalação de atualizações

A disponibilidade deste recurso depende do modo do Kaspersky Security Center Cloud Console e da licença atual.

Para criar uma tarefa para instalar atualizações de softwares de terceiros usando o assistente de Instalação de atualizações:

1. No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Atualizações de software**.

Aparece uma lista das atualizações disponíveis.

2. Marque a caixa de seleção ao lado da atualização que deseja instalar.

3. Clique no botão **Executar o Assistente de Instalação de Atualização**.

   O assistente de Instalação de atualizações é iniciado. A página **Selecionar tarefa de instalação da atualização** exibe a lista de todas as tarefas existentes dos seguintes tipos:

   - *Instalar as atualizações necessárias e corrigir vulnerabilidades*
   - *Instalar as atualizações do Windows Update*
   - *Corrigir vulnerabilidades*

   Você não pode modificar as tarefas dos dois últimos tipos para instalar novas atualizações. Para instalar novas atualizações, você só pode usar as tarefas do tipo *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

4. Caso deseje que o assistente exiba apenas as tarefas que instalam a atualização selecionada, ative a opção **Exibir apenas tarefas que instalam esta atualização**.

5. Selecione o que deseja fazer:

   - Para iniciar uma tarefa, marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Iniciar**.
   - Para adicionar uma nova regra a uma tarefa existente:

     a. Marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Adicionar regra**.

     b. Na página aberta, configure a nova regra:

     - Regra de instalação de atualizações deste nível de importância

       Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

       Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

       Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

       Por padrão, esta opção está desativada.

     - Regra de instalação de atualizações deste nível de importância de acordo com o MSRC (disponível apenas para atualizações do Windows Update)

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada (disponível apenas para atualizações do Windows Update), as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

Por padrão, esta opção está desativada.

- Regra de instalação para atualizações deste fornecedor (disponível apenas para atualizações de aplicativos de terceiros)

  Esta opção está disponível apenas para atualizações de aplicativos de terceiros. O Kaspersky Security Center Cloud Console instala apenas as atualizações relacionadas aos aplicativos feitos pelo mesmo fornecedor que a atualização selecionada. As atualizações recusadas e as atualizações dos aplicativos feitos por outros fornecedores não são instaladas.

  Por padrão, esta opção está desativada.

- **Regra de instalação para atualizações do tipo**

- **Regra de instalação para a atualização selecionada**

- Aprovar atualizações selecionadas

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

- Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas

  Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

  Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

  Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

  Por padrão, esta opção está ativada.

c. Clique no botão **Adicionar**.

- Para criar uma tarefa:

a. Clique no botão **Nova tarefa**.

b. Na página aberta, configure a nova regra:

- **Regra de instalação de atualizações deste nível de importância**

  Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

  Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

  Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

  Por padrão, esta opção está desativada.

- **Regra de instalação de atualizações deste nível de importância de acordo com o MSRC** (disponível apenas para atualizações do Windows Update)

  Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

  Se esta opção estiver ativada (disponível apenas para atualizações do Windows Update), as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

  Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

  Por padrão, esta opção está desativada.

- **Regra de instalação para atualizações deste fornecedor** (disponível apenas para atualizações de aplicativos de terceiros)

  Esta opção está disponível apenas para atualizações de aplicativos de terceiros. O Kaspersky Security Center Cloud Console instala apenas as atualizações relacionadas aos aplicativos feitos pelo mesmo fornecedor que a atualização selecionada. As atualizações recusadas e as atualizações dos aplicativos feitos por outros fornecedores não são instaladas.

  Por padrão, esta opção está desativada.

- **Regra de instalação para atualizações do tipo**

- **Regra de instalação para a atualização selecionada**

- **Aprovar atualizações selecionadas**

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

- **Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas**

  Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

  Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

  Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

  Por padrão, esta opção está ativada.

c. Clique no botão **Adicionar**.

Se você optou por iniciar uma tarefa, poderá fechar o assistente. A tarefa será concluída no modo de segundo plano. Nenhuma outra ação será necessária.

Se você escolheu adicionar uma regra a uma tarefa existente, a janela de propriedades da tarefa é aberta. A nova regra já foi adicionada às propriedades da tarefa. Você pode visualizar ou modificar a regra ou outras configurações de tarefa. Clique no botão **Salvar** para salvar as alterações.

Caso tenha optado por criar uma tarefa, continue a criar a tarefa no assistente para Novas tarefas. A nova regra adicionada no assistente de Instalação de atualizações é exibida no Assistente para Novas Tarefas. Ao concluir o assistente para novas tarefas, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é adicionada à lista de tarefas.

Criar a tarefa Encontrar vulnerabilidades e atualizações necessárias

Por meio da tarefa Encontrar as vulnerabilidades e as atualizações necessárias, o Kaspersky Security Center Cloud Console recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para o software de terceiro instalado nos dispositivos gerenciados.

A tarefa Encontrar as vulnerabilidades e as atualizações necessárias é criada automaticamente quando o Assistente de Início Rápido é executado. Caso não tenha executado o assistente, é possível criar a tarefa manualmente.

Para criar uma tarefa Encontrar as vulnerabilidades e as atualizações necessárias:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center Cloud Console, selecione o tipo de tarefa **Encontrar as vulnerabilidades e as atualizações necessárias**.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

5. Dispositivos aos quais a tarefa será atribuída.

6. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

7. Clique no botão **Criar**.

   A tarefa é criada e exibida na lista de tarefas.

8. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

9. Na janela Propriedades da tarefa, especifique as configurações gerais da tarefa.

10. Na guia **Configurações do aplicativo**, especifique as seguintes configurações:

    - **Buscar por vulnerabilidades e atualizações listadas pela Microsoft**

      Ao procurar vulnerabilidades e atualizações, o Kaspersky Security Center Cloud Console usa as informações sobre atualizações aplicáveis da Microsoft a partir da fonte de atualizações da Microsoft disponíveis no momento.

      Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft e atualizações de aplicativos de terceiros.

      Por padrão, esta opção está ativada.

    - **Conectar com o servidor de atualizações para atualizar dados**

O Windows Update Agent em um dispositivo gerenciado se conecta à fonte das atualizações da Microsoft. Os seguintes servidores podem atuar como uma fonte de atualizações da Microsoft:

- Servidor de Administração do Kaspersky Security Center Cloud Console (consulte as Configurações da política do Agente de Rede)
- Windows Server com o WSUS (Microsoft Windows Server Update Services) implementado na rede da sua organização
- Servidores de atualizações da Microsoft

Se esta opção estiver ativada, o Windows Update Agent em um dispositivo gerenciado se conecta à fonte de atualizações da Microsoft para atualizar as informações sobre as atualizações do Microsoft Windows aplicáveis.

Se esta opção estiver desativada, o Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações do Microsoft Windows aplicáveis recebidas da fonte de atualizações da Microsoft anteriormente e que estão armazenadas no cache do dispositivo.

A conexão à fonte de atualizações da Microsoft pode consumir muitos recursos. Você pode desativar esta opção se definir a conexão regular com esta fonte de atualizações em outra tarefa ou nas propriedades da política do Agente de Rede, na seção **Atualizações e vulnerabilidades de software**. Se não deseja desativar essa opção, para reduzir a sobrecarga no servidor, você pode configurar o agendamento da tarefa para atrasar aleatoriamente o início da tarefa em 360 minutos.

Por padrão, esta opção está ativada.

A combinação das seguintes opções das configurações da política do Agente de Rede define o modo de obter atualizações:

- O Windows Update Agent em um dispositivo gerenciado se conecta ao servidor de atualizações para obter atualizações somente se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Ativo** no grupo de configurações no modo **Modo de pesquisa do Windows Update** é selecionado.
- O Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações aplicáveis do Microsoft Windows que foram recebidas da fonte de atualizações da Microsoft anteriormente e armazenadas no cache do dispositivo, se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Passivo**, no grupo de configurações **Modo de pesquisa do Windows Update**, estiver selecionada, ou se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Ativo**, no grupo de configurações **Modo de pesquisa do Windows Update**, estiver selecionada.
- Independentemente do status da opção **Conectar com o servidor de atualizações para atualizar dados** (ativado ou desativado), se a opção **Desativado** no grupo de configurações no modo **Modo de pesquisa do Windows Update** estiver selecionada, o Kaspersky Security Center Cloud Console não solicita nenhuma informação sobre atualizações.

- Buscar por vulnerabilidades e atualizações de terceiros, listadas pela Kaspersky

Se esta opção estiver ativada, o Kaspersky Security Center Cloud Console pesquisará vulnerabilidades e atualizações necessárias em aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft) no Registro do Windows e nas pastas especificadas em **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**. A lista completa de suporte a aplicativos de terceiros é gerenciada pela Kaspersky.

Se esta opção estiver desativada, o Kaspersky Security Center Cloud Console não procurará vulnerabilidades e atualizações necessárias de aplicativos de terceiros. Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft Windows e atualizações de aplicativos de terceiros.

Por padrão, esta opção está ativada.

- **Especifique caminhos para a pesquisa avançada de aplicativos no sistema de arquivos**

  As pastas nas quais o Kaspersky Security Center Cloud Console pesquisa aplicativos de terceiros que necessitem de correção de vulnerabilidades e de instalação de atualizações. Você pode usar variáveis de sistema.

  Especifique as pastas nas quais os aplicativos são instalados. Por padrão, a lista está vazia.

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará rastreamentos, mesmo se o rastreamento estiver desativado para o Agente de Rede no Utilitário de diagnóstico remoto do Kaspersky Security Center Cloud Console. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a gravar neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se este recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center Cloud Console. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

11. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Se os resultados da tarefa contiverem um aviso do erro 0x80240033 "Erro de atualização do Windows Update Agent 80240033 ("Não foi possível baixar os termos da licença.")", você poderá resolver esse problema no Registro do Windows.

As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias

A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente quando o Assistente de Início Rápido é executado. Caso não tenha executado o assistente, é possível criar a tarefa manualmente.

Além das configurações gerais da tarefa, é possível especificar as seguintes configurações ao criar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou mais recentes, ao configurar as propriedades da tarefa criada:

- **Buscar por vulnerabilidades e atualizações listadas pela Microsoft**

  Ao procurar vulnerabilidades e atualizações, o Kaspersky Security Center Cloud Console usa as informações sobre atualizações aplicáveis da Microsoft a partir da fonte de atualizações da Microsoft disponíveis no momento.

  Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft e atualizações de aplicativos de terceiros.

  Por padrão, esta opção está ativada.

- **Conectar com o servidor de atualizações para atualizar dados**

O Windows Update Agent em um dispositivo gerenciado se conecta à fonte das atualizações da Microsoft. Os seguintes servidores podem atuar como uma fonte de atualizações da Microsoft:

- Servidor de Administração do Kaspersky Security Center Cloud Console (consulte as Configurações da política do Agente de Rede)
- Windows Server com o WSUS (Microsoft Windows Server Update Services) implementado na rede da sua organização
- Servidores de atualizações da Microsoft

Se esta opção estiver ativada, o Windows Update Agent em um dispositivo gerenciado se conecta à fonte de atualizações da Microsoft para atualizar as informações sobre as atualizações do Microsoft Windows aplicáveis.

Se esta opção estiver desativada, o Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações do Microsoft Windows aplicáveis recebidas da fonte de atualizações da Microsoft anteriormente e que estão armazenadas no cache do dispositivo.

A conexão à fonte de atualizações da Microsoft pode consumir muitos recursos. Você pode desativar esta opção se definir a conexão regular com esta fonte de atualizações em outra tarefa ou nas propriedades da política do Agente de Rede, na seção **Atualizações e vulnerabilidades de software**. Se não deseja desativar essa opção, para reduzir a sobrecarga no servidor, você pode configurar o agendamento da tarefa para atrasar aleatoriamente o início da tarefa em 360 minutos.

Por padrão, esta opção está ativada.

A combinação das seguintes opções das configurações da política do Agente de Rede define o modo de obter atualizações:

- O Windows Update Agent em um dispositivo gerenciado se conecta ao servidor de atualizações para obter atualizações somente se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Ativo** no grupo de configurações no modo **Modo de pesquisa do Windows Update** é selecionado.
- O Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações aplicáveis do Microsoft Windows que foram recebidas da fonte de atualizações da Microsoft anteriormente e armazenadas no cache do dispositivo, se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Passivo**, no grupo de configurações **Modo de pesquisa do Windows Update**, estiver selecionada, ou se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Ativo**, no grupo de configurações **Modo de pesquisa do Windows Update**, estiver selecionada.
- Independentemente do status da opção **Conectar com o servidor de atualizações para atualizar dados** (ativado ou desativado), se a opção **Desativado** no grupo de configurações no modo **Modo de pesquisa do Windows Update** estiver selecionada, o Kaspersky Security Center Cloud Console não solicita nenhuma informação sobre atualizações.

- Buscar por vulnerabilidades e atualizações de terceiros, listadas pela Kaspersky

Se esta opção estiver ativada, o Kaspersky Security Center Cloud Console pesquisará vulnerabilidades e atualizações necessárias em aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft) no Registro do Windows e nas pastas especificadas em **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**. A lista completa de suporte a aplicativos de terceiros é gerenciada pela Kaspersky.

Se esta opção estiver desativada, o Kaspersky Security Center Cloud Console não procurará vulnerabilidades e atualizações necessárias de aplicativos de terceiros. Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft Windows e atualizações de aplicativos de terceiros.

Por padrão, esta opção está ativada.

- **Especifique caminhos para a pesquisa avançada de aplicativos no sistema de arquivos**

  As pastas nas quais o Kaspersky Security Center Cloud Console pesquisa aplicativos de terceiros que necessitem de correção de vulnerabilidades e de instalação de atualizações. Você pode usar variáveis de sistema.

  Especifique as pastas nas quais os aplicativos são instalados. Por padrão, a lista está vazia.

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará rastreamentos, mesmo se o rastreamento estiver desativado para o Agente de Rede no Utilitário de diagnóstico remoto do Kaspersky Security Center Cloud Console. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a gravar neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se este recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center Cloud Console. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

Recomendações sobre o agendamento de tarefas

Ao agendar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*, certifique-se de que as duas opções **Executar tarefas ignoradas** e **Usar atraso aleatório automaticamente para início da tarefa** estejam desativadas.

Por padrão, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é configurada para iniciar manualmente. Caso as regras do local de trabalho da organização ofereçam o desligamento de todos os dispositivos nessa hora, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* será executada após os dispositivos serem ligados novamente, ou seja, na manhã do dia seguinte. Tal atividade pode ser indesejável porque uma verificação de vulnerabilidades pode aumentar a carga de subsistemas de disco e da CPU. Você deve definir o agendamento mais conveniente para a tarefa com base nas regras do local de trabalho adotadas na organização.

Criar a tarefa Instalar atualizações necessárias e corrigir vulnerabilidades

A disponibilidade da tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* depende do modo Kaspersky Security Center Cloud Console e da licença atual.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa permite instalar várias atualizações e corrigir várias vulnerabilidades, de acordo com determinadas regras.

Para instalar atualizações ou corrigir vulnerabilidades usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, execute uma das seguintes ações:

- Execute o assistente de Instalação das atualizações ou o assistente para Correção de vulnerabilidades.
- Crie uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.
- Adicione uma regra para instalação da atualização a uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.

As tarefas de instalação da atualização de software têm uma série de limitações. Essas limitações dependem da licença sob a qual você está usando o Kaspersky Security Center Cloud Console e do modo em que o Kaspersky Security Center Cloud Console está operando.

Para criar uma tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center Cloud Console, selecione o tipo de tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades**.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.
6. Especifique as regras para instalação da atualização e, então, especifique as seguintes configurações:
   - **Iniciar a instalação ao reiniciar ou fechar o dispositivo**

Se esta opção estiver ativada, as atualizações serão instaladas quando o dispositivo for reiniciado ou desligado. Caso contrário, as atualizações são instaladas segundo o agendamento.

Use esta opção caso a instalação das atualizações afete o desempenho do dispositivo.

Por padrão, esta opção está desativada.

- **Instalar os componentes gerais do sistema necessários**

  Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional

  Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

  Por padrão, esta opção está desativada.

- **Permitir a instalação de novas versões dos aplicativos durante atualizações**

  Se esta opção estiver ativada, as atualizações serão permitidas quando resultarem na instalação de uma nova versão de um aplicativo de software.

  Se esta opção estiver desativada, o software não será atualizado. Você poderá então instalar novas versões do software manualmente ou através de outra tarefa. Por exemplo, você pode usar esta opção se a infraestrutura da sua empresa não tiver como base uma nova versão do software ou se você quiser verificar uma atualização usando uma infraestrutura de teste.

  Por padrão, esta opção está ativada.

  A atualização de um aplicativo pode causar o funcionamento incorreto de aplicativos dependentes instalados em dispositivos cliente.

- **Baixar atualizações para o dispositivo sem instalá-las**

  Se esta opção estiver ativada, o aplicativo baixa as atualizações em um dispositivo cliente, mas não as instala automaticamente. Você então poderá instalar manualmente as atualizações baixadas.

  As atualizações da Microsoft são baixadas no armazenamento de sistema do Windows. Atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencentes à Kaspersky e à Microsoft) são baixados na pasta especificada no campo **Baixar atualizações para**.

  Se esta opção estiver desativada, as atualizações serão instaladas no dispositivo automaticamente.

  Por padrão, esta opção está desativada.

- **Pasta para download de atualizações**

  Esta pasta é usada para baixar atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft).

- **Ativar diagnóstico avançado**

Se este recurso estiver ativado, o Agente de Rede gravará rastreamentos, mesmo se o rastreamento estiver desativado para o Agente de Rede no Utilitário de diagnóstico remoto do Kaspersky Security Center Cloud Console. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a gravar neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

Se este recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center Cloud Console. Nenhum rastreamento adicional é gravado.

Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

7. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Tempo de espera antes do fechamento forçado de aplicativos nas sessões bloqueadas (min)**

  Os aplicativos são fechados no modo forçado quando o dispositivo for bloqueado (automaticamente, após um intervalo especificado de inatividade ou manualmente).

  Se esta opção estiver ativada, os aplicativos serão forçados a fechar no dispositivo bloqueado após a expiração do intervalo de tempo especificado no campo de entrada.

  Se essa opção estiver ativada, os aplicativos não serão fechados no dispositivo bloqueado.

  Por padrão, esta opção está desativada.

8. Se na página **Concluir a criação da tarefa**, você ativar a opção **Abrir detalhes da tarefa quando a criação for concluída**, você pode modificar as configurações padrão da tarefa. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.

10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

11. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

12. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

Se os resultados da tarefa contiverem um aviso do erro 0x80240033 "Erro de atualização do Windows Update Agent 80240033 ("Não foi possível baixar os termos da licença.")", você poderá resolver esse problema no Registro do Windows.

Adicionar regras para instalação da atualização

A disponibilidade deste recurso depende do modo do Kaspersky Security Center Cloud Console e da licença atual.

Ao instalar atualizações de software ou corrigir vulnerabilidades de software usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é necessário especificar regras para a instalação da atualização. Essas regras determinam as atualizações a serem instaladas e as vulnerabilidades a serem corrigidas.

As configurações exatas dependem de você ter adicionado uma regra para todas as atualizações, para atualizações do Windows Update ou para atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software que não sejam a Kaspersky ou a Microsoft). Ao adicionar uma regra para atualizações do Windows Update ou atualizações de aplicativos de terceiros, é possível selecionar aplicativos e versões de aplicativo específicos para os quais deseja instalar atualizações. Ao adicionar uma regra para todas as atualizações, é possível selecionar atualizações específicas que deseja instalar e vulnerabilidades que deseja corrigir com a instalação das atualizações.

É possível adicionar uma regra para a instalação da atualização das seguintes maneiras:

- Adicionando uma regra ao criar uma nova tarefa do tipo Instalar as atualizações necessárias e corrigir vulnerabilidades.
- Adicionando uma regra na guia **Configurações do aplicativo** na janela de propriedades de uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.
- Por meio do assistente de Instalação das atualizações ou do assistente para Correção de vulnerabilidades.

Para adicionar uma nova regra para todas as atualizações:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para todas as atualizações**.

3. Na página **Critérios gerais**, use as listas suspensas para especificar as seguintes configurações:

   - **Conjunto de atualizações a instalar**

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:
     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - **Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que**

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

Por padrão, esta opção está desativada.

4. Na página **Atualizações**, selecione as atualizações a serem instaladas:

- **Instalar todas as atualizações adequadas**

  Instale todas as atualizações de software que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Instalar apenas as atualizações da lista**

  Instale somente as atualizações de software que você seleciona manualmente da lista. Essa lista contém todas as atualizações de software disponíveis.

  Por exemplo, pode ser necessário selecionar atualizações específicas nos seguintes casos: para verificar a instalação em um ambiente de teste, para atualizar somente aplicativos críticos ou para atualizar somente aplicativos específicos.

- **Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas**

  Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

  Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

  Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

  Por padrão, esta opção está ativada.

5. Na página **Vulnerabilidades**, selecione as vulnerabilidades que serão corrigidas instalando as atualizações selecionadas:

- **Corrigir todas as vulnerabilidades que correspondem a outros critérios**

  Corrija todas as vulnerabilidades que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Corrigir somente vulnerabilidades da lista**

Corrija somente as vulnerabilidades que você seleciona manualmente da lista. Essa lista contém todas as vulnerabilidades detectadas.

Por exemplo, pode ser necessário selecionar vulnerabilidades específicas nos seguintes casos: para verificar a correção em um ambiente de teste, para corrigir vulnerabilidades somente em aplicativos críticos ou para corrigir vulnerabilidades somente em aplicativos específicos.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Para adicionar uma nova regra para atualizações do Windows Update:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para o Windows Update**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

- Conjunto de atualizações a instalar

  Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

  - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
  - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
  - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

- Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

  Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

  Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

  Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

  Por padrão, esta opção está desativada.

- Corrigir vulnerabilidades com um nível de gravidade do MSRC igual ou maior do que

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Categorias de atualizações**, selecione as categorias das atualizações a serem instaladas. Essas categorias são iguais às no Catálogo do Microsoft Update. Por padrão, todas as categorias estão selecionadas.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Para adicionar uma nova regra para as atualizações de aplicativos de terceiros:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para atualizações de terceiros**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção Configurações da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Criar a tarefa Instalar atualizações do Windows Update

A tarefa Instalar atualizações do Windows Update permite instalar atualizações de software fornecidas pelo serviço Windows Update em dispositivos cliente.

As tarefas de instalação da atualização de software têm uma série de limitações. Essas limitações dependem da licença sob a qual você está usando o Kaspersky Security Center Cloud Console e do modo em que o Kaspersky Security Center Cloud Console está operando.

Para criar a tarefa Instalar atualizações do Windows Update:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.

2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Para o aplicativo Kaspersky Security Center Cloud Console, selecione o tipo de tarefa **Instalar as atualizações do Windows Update**.

4. Especifique o nome da tarefa que está criando.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).

5. Dispositivos aos quais a tarefa será atribuída.

6. Clique no botão **Adicionar**.

   A lista de atualizações é aberta.

7. Selecione as atualizações do Windows Update que deseja instalar e, a seguir, clique em **OK**.

8. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

9. Especificar as configurações da conta:

- **Conta padrão**

  A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

  Por padrão, esta opção está selecionada.

- **Especificar conta**

  Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

- **Conta**

  Conta sob a qual a tarefa é executada.

- **Senha**

  Senha da conta sob a qual a tarefa será executada.

10. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

11. Clique no botão **Concluir**.

    A tarefa é criada e exibida na lista de tarefas.

12. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

13. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

14. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Exibir informações sobre atualizações disponíveis para software de terceiros

Você pode visualizar a lista de atualizações disponíveis para software de terceiros, incluindo software da Microsoft, instalado em dispositivos cliente.

Para exibir uma lista de atualizações disponíveis para aplicativos de terceiros instalados em dispositivos cliente,

No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Atualizações de software**.

Aparece uma lista das atualizações disponíveis.

Você pode especificar um filtro para visualizar a lista de atualizações de software. Clique no ícone **Filtro** () no canto superior direito da lista de atualizações de software para gerenciar o filtro. Você também pode selecionar um dos filtros predefinidos na lista suspensa **Filtros predefinidos** acima da lista de vulnerabilidades de software.

Para visualizar as propriedades de uma atualização:

1. Clique no nome da atualização de software necessária.
2. A janela de propriedades da atualização é aberta, exibindo informações agrupadas nas seguintes guias:

- **Geral**

  Esta guia exibe detalhes gerais da atualização selecionada:

  - Status de aprovação da atualização (pode ser alterado manualmente, selecionando um novo status na lista suspensa)
  - Categoria do Windows Server Update Services (WSUS) à qual a atualização pertence
  - Data e hora em que a atualização foi registrada
  - Data e hora em que a atualização foi criada
  - Nível de importância da atualização
  - Requisitos de instalação impostos pela atualização
  - Família de aplicativos à qual a atualização pertence
  - Aplicativo ao qual a atualização se aplica
  - Número da revisão de atualização

- **Atributos**

Esta guia exibe um conjunto de atributos que você pode usar para obter mais informações sobre a atualização selecionada. Este conjunto difere, dependendo se a atualização é publicada pela Microsoft ou por um fornecedor terceiro.

A guia exibe as seguintes informações para uma atualização da Microsoft:

- O nível de importância da atualização, conforme definido pelo Microsoft Security Response Center (MSRC)
- Link para o artigo na Base de Dados de Conhecimento Microsoft que descreve a atualização
- Link para o artigo no Boletim de Segurança da Microsoft que descreve a atualização
- Identificador da atualização (ID)

A guia exibe as seguintes informações para uma atualização de terceiros:

- Se a atualização é um patch ou um pacote de distribuição completo
- Idioma de localização da atualização
- Se a atualização é instalada automática ou manualmente
- Se a atualização foi revogada após ser aplicada
- Link para baixar a atualização

- **Dispositivos**

  Esta guia exibe uma lista de dispositivos nos quais a atualização selecionada foi instalada.

- **Vulnerabilidades corrigidas**

  Esta guia exibe uma lista de vulnerabilidades que a atualização selecionada pode corrigir.

- **Cruzamento de atualizações**

  Esta guia exibe possíveis redundâncias entre várias atualizações publicadas para o mesmo aplicativo, ou seja, se a atualização selecionada pode substituir outras atualizações ou, vice-versa (disponíveis apenas para atualizações Windows).

- **Tarefas para instalar esta atualização**

  Esta guia exibe uma lista de tarefas cujo escopo inclui a instalação da atualização selecionada. A guia também permite que você crie uma nova tarefa de instalação remota para a atualização.

Para exibir as estatísticas de uma instalação de atualização:

1. Selecione a caixa de seleção ao lado da atualização de software necessária.
2. Clique no botão **Estatísticas de status da instalação de atualizações**.

O diagrama dos status de instalação da atualização é exibido. Clicar em um status abre uma lista de dispositivos nos quais a atualização tem o status selecionado.

Você pode visualizar informações sobre atualizações de software disponíveis para software de terceiros, incluindo software da Microsoft, instalado no dispositivo gerenciado selecionado que executa o Windows.

Para visualizar uma lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo para o qual você deseja visualizar atualizações de software de terceiros.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Na janela de propriedades do dispositivo selecionado selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Atualizações disponíveis**. Caso deseje visualizar apenas as atualizações instaladas, ative a opção **Exibir atualizações instaladas**.

A lista de atualizações de software de terceiros disponíveis para o dispositivo selecionado é exibida.

Exportando a lista de vulnerabilidades de software para um arquivo

Você pode exportar a lista de atualizações para software de terceiros, incluindo o software Microsoft, exibido no momento para os arquivos CSV e TXT. Você pode usar esses arquivos, por exemplo, para enviá-los ao seu gerente de segurança de informações ou para armazená-los para fins de estatística.

Para exportar como arquivo de texto a lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Atualizações de software**.

   A página exibe uma lista de atualizações disponíveis para software de terceiros instalado em todos os dispositivos gerenciados.

2. Clique no botão **Exportar para TXT** ou **Exportar para CSV**, dependendo do formato de exportação preferido.

O arquivo contendo a lista de atualizações para software de terceiros, incluindo software da Microsoft, é baixado para o dispositivo usado no momento.

Para exportar como arquivo de texto uma lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:

1. Abra a lista de atualizações de software de terceiros disponíveis no dispositivo gerenciado selecionado.

2. Selecione as atualizações de software que você deseja exportar.

   Ignore esta etapa se desejar exportar uma lista completa de atualizações de software.

   Se você deseja exportar a lista completa de atualizações de software, apenas as vulnerabilidades exibidas na página atual serão exportadas.

   Se deseja exportar apenas as atualizações instaladas, marque a caixa **Exibir atualizações instaladas**.

3. Clique no botão **Exportar para TXT** ou **Exportar para CSV**, dependendo do formato de exportação preferido.

O arquivo contendo a lista de atualizações para software de terceiros, incluindo software da Microsoft, instalados no dispositivo gerenciado é baixado para o dispositivo usado no momento.

Aprovando e recusando atualizações de software de terceiros

Ao configurar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é possível criar uma regra que exija um status específico das atualizações a serem instaladas. Por exemplo, uma regra de atualização pode permitir a instalação do seguinte:

- Somente atualizações aprovadas
- Somente atualizações aprovadas e indefinidas
- Todas as atualizações, independentemente dos status de atualização

Você pode aprovar atualizações que devem ser instaladas e recusar as atualizações que não devem ser instaladas.

O uso do status *Aprovado* para gerenciar a instalação da atualização é eficiente para uma pequena quantidade de atualizações. Para instalar várias atualizações, use as regras que você pode configurar na tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades*. Recomendamos que você defina o status *Aprovado* apenas para as atualizações específicas que não atendem aos critérios especificados nas regras. Ao aprovar manualmente uma grande quantidade de atualizações, o desempenho do Servidor de Administração é reduzido, o que pode levar à sua sobrecarga.

Para aprovar ou recusar uma ou várias atualizações:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Atualizações de software**.

   Aparece uma lista das atualizações disponíveis.

2. Selecione as atualizações que deseja aprovar ou recusar.

3. Clique em **Aprovar** para aprovar as atualizações selecionadas ou **Recusar** para recusar as atualizações selecionadas.

   O valor padrão é *Indefinido*.

As atualizações selecionadas têm os status que você definiu.

Como opção, você pode alterar o status de aprovação nas propriedades de uma atualização específica.

Para aprovar ou recusar uma atualização em suas propriedades:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Atualizações de software**.

   Aparece uma lista das atualizações disponíveis.

2. Clique no nome da atualização que deseja aprovar ou recusar.

   A janela Propriedades da atualização é aberta.

3. Na seção **Geral**, selecione um status para a atualização, alterando a opção **Status de aprovação da atualização**. Você pode selecionar o status *Aprovado*, *Negado*, ou *Indefinido*.

4. Clique no botão **Salvar** para salvar as alterações.

A atualização selecionada tem o status que você definiu.

Se você definir o status **Negado** para atualizações de software de terceiros, estas atualizações não serão instaladas em dispositivos para os quais elas foram planejadas, mas que ainda não foram instaladas. As atualizações permanecerão nos dispositivos nos quais elas já foram instaladas. Se você tiver de excluí-las, poderá excluí-las manualmente localmente.

Atualizar aplicativos de terceiros automaticamente

Alguns aplicativos de terceiros podem ser atualizados automaticamente. O fornecedor do aplicativo define se o aplicativo é compatível ou não com o recurso de atualização automática. Se um aplicativo de terceiros instalado em um dispositivo gerenciado for compatível com atualização automática, você poderá especificar a configuração de atualização automática nas propriedades do aplicativo. Depois de alterar a configuração de atualização automática, os Agentes de Rede aplicam a nova configuração a cada dispositivo gerenciado no qual o aplicativo está instalado.

A configuração de atualização automática é independente dos outros objetos e configurações do recurso Gerenciamento de patches e vulnerabilidades. Por exemplo, esta configuração não depende de um status de aprovação de atualização ou das tarefas de instalação da atualização, como *Instalar as atualizações necessárias e corrigir vulnerabilidades*, *Instalar as atualizações do Windows Update* e *Corrigir vulnerabilidades*.

Para definir a configuração de atualização automática para um aplicativo de terceiros:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos**.
2. Clique no nome do aplicativo para o qual deseja alterar a configuração de atualização automática.

   Para simplificar a pesquisa, você pode filtrar a lista pela coluna **Status das atualizações automáticas**.

   A janela Propriedades do aplicativo é aberta.
3. Na seção **Geral**, selecione um valor para a seguinte configuração:

   Status das atualizações automáticas

Selecione uma das seguintes opções:

- **Indefinido**

  O recurso de atualização automática será desativado. O Kaspersky Security Center Cloud Console instala atualizações de aplicativos de terceiros usando as tarefas: *Instalar as atualizações necessárias e corrigir vulnerabilidades*, *Instalar as atualizações do Windows Update* e *Corrigir vulnerabilidades*.

- **Permitido**

  Depois que o fornecedor lança uma atualização para o aplicativo, esta atualização é instalada nos dispositivos gerenciados automaticamente. Nenhuma outra ação é necessária.

- **Bloqueado**

  As atualizações do aplicativo não são instaladas automaticamente. O Kaspersky Security Center Cloud Console instala atualizações de aplicativos de terceiros usando as tarefas: *Instalar as atualizações necessárias e corrigir vulnerabilidades*, *Instalar as atualizações do Windows Update* e *Corrigir vulnerabilidades*.

4. Clique no botão **Salvar** para salvar as alterações.

A configuração de atualização automática é aplicada ao aplicativo selecionado.

Corrigindo vulnerabilidades de software de terceiros

Esta seção descreve os recursos do Kaspersky Security Center Cloud Console relacionados à correção de vulnerabilidades no software instalado nos dispositivos gerenciados.

Cenário: Localizar e corrigir vulnerabilidades de software

Esta seção fornece um cenário para localizar e corrigir vulnerabilidades nos dispositivos gerenciados que executam o Windows. Você pode encontrar e corrigir vulnerabilidades de software no sistema operacional e em software de terceiros, incluindo software da Microsoft.

Pré-requisitos

- O Kaspersky Security Center Cloud Console está implementado em sua organização.
- Há dispositivos gerenciados executando o Windows na sua organização.

Fases

A localização e a correção de vulnerabilidades de software ocorre em fases:

1. **Verificar vulnerabilidades no software instalado nos dispositivos cliente**

Para encontrar vulnerabilidades no software instalado nos dispositivos gerenciados, execute a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Kaspersky Security Center Cloud Console recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa.

A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center Cloud Console. Caso não tenha executado o assistente, inicie-o agora ou crie a tarefa manualmente.

Instruções: Creating the Encontrar as vulnerabilidades e as atualizações necessárias task

2 Analisar a lista de vulnerabilidades de software detectadas

Visualize a lista **Vulnerabilidades de software** e decida quais vulnerabilidades devem ser corrigidas. Para visualizar informações detalhadas sobre cada vulnerabilidade, clique no nome da vulnerabilidade na lista. Para cada vulnerabilidade na lista, você também pode visualizar as estatísticas sobre a vulnerabilidade nos dispositivos gerenciados.

Instruções de como proceder:

- Exibir informações sobre as vulnerabilidades do software
- Visualizar as estatísticas de vulnerabilidades em dispositivos gerenciados

3 Configurar a correção de vulnerabilidades

Quando as vulnerabilidades de software são detectadas, é possível corrigi-las nos dispositivos gerenciados usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa permite instalar várias atualizações e corrigir várias vulnerabilidades, de acordo com determinadas regras. A disponibilidade desta tarefa depende do modo do Kaspersky Security Center Cloud Console e de sua licença atual. Para corrigir vulnerabilidades de software, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* usa as atualizações de software recomendadas.

A tarefa *Corrigir vulnerabilidades* usa correções recomendadas para softwares da Microsoft.

É possível iniciar o Assistente para Correção de Vulnerabilidades, que cria uma dessas tarefas automaticamente, ou criá-las manualmente.

Instruções sobre como proceder: Corrigir vulnerabilidades em software de terceiros, Criar a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades

4 Agendar as tarefas

Para garantir que a lista de vulnerabilidades esteja sempre atualizada, agende a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para executá-la automaticamente de tempo em tempo. A frequência média recomendada é de uma vez por semana.

Se você criou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, pode agendá-la para ser executada com a mesma frequência que a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou com menor frequência. Ao agendar a tarefa *Corrigir vulnerabilidades*, é necessário selecionar as correções para softwares da Microsoft sempre antes de iniciar a tarefa.

Ao agendar as tarefas, certifique-se que uma tarefa para corrigir vulnerabilidades é iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

5 Ignorar vulnerabilidades de software (opcional)

Se você desejar, poderá ignorar as vulnerabilidades de software a ser corrigidas em todos os dispositivos gerenciados ou apenas nos dispositivos gerenciados selecionados.

Instruções de como proceder: Ignorar vulnerabilidades de software

6. **Executando uma tarefa de correção de vulnerabilidades**

   Inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*. Após a conclusão da tarefa, verifique se ela possui o status *Concluída com êxito* na lista de tarefas.

7. **Criar o relatório sobre os resultados da correção de vulnerabilidades de software (opcional)**

   Para ver estatísticas detalhadas sobre a correção de vulnerabilidades, gere um Relatório de vulnerabilidades. O relatório exibe informações sobre vulnerabilidades de software que não são corrigidas. Assim, é possível ter uma ideia sobre como encontrar e corrigir vulnerabilidades em softwares de terceiros, incluindo softwares da Microsoft, em sua organização.

   Instruções de como proceder: Gerar e visualizar um relatório

8. **Verificar a configuração para encontrar e corrigir vulnerabilidades em software de terceiros**

   Certifique-se do seguinte:

   - A lista de vulnerabilidades de software em dispositivos gerenciados não está vazia.
   - Uma tarefa para corrigir as vulnerabilidades encontra-se na lista de tarefas.
   - As tarefas para encontrar e corrigir vulnerabilidades de software estão agendadas, de modo que são iniciadas sequencialmente. Veja as propriedades dessas tarefas e compare o agendamento.
   - A tarefa de corrigir vulnerabilidades de software foi concluída com êxito. Visualize as informações na guia **Resultados** da janela de propriedades da tarefa.

Resultados

Se você criou e configurou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, as vulnerabilidades são corrigidas nos dispositivos gerenciados automaticamente. Quando a tarefa é executada, ela correlaciona a lista de atualizações de software disponíveis às regras especificadas nas configurações da tarefa. Todas as atualizações de software que atendem aos critérios das regras serão baixadas no repositório dos pontos de distribuição e instaladas para corrigir as vulnerabilidades de software.

Se você criou a tarefa *Corrigir vulnerabilidades*, apenas as vulnerabilidades de software no software da Microsoft são corrigidas.

Sobre como encontrar e corrigir vulnerabilidades de software

O Kaspersky Security Center Cloud Console detecta e corrige vulnerabilidades de software em dispositivos gerenciados que executam os sistemas operacionais das famílias Microsoft Windows. As vulnerabilidades são detectadas no sistema operacional e no software de terceiros, incluindo o software da Microsoft.

Localizar vulnerabilidades de software

Para encontrar vulnerabilidades de software, o Kaspersky Security Center Cloud Console usa características do banco de dados de vulnerabilidades conhecidas Windows Update Database. Este banco de dados de vulnerabilidades conhecidas é criado e mantido por especialistas da Kaspersky. Ele contém informações sobre vulnerabilidades, como descrição da vulnerabilidade, data de detecção da vulnerabilidade, nível de gravidade da vulnerabilidade. Você pode encontrar os detalhes das vulnerabilidades de software no site da Kaspersky.

O Kaspersky Security Center Cloud Console usa a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para encontrar vulnerabilidades de software.

Corrigir vulnerabilidades de software

Para corrigir vulnerabilidades de software, o Kaspersky Security Center Cloud Console usa atualizações de software emitidas pelos fornecedores do software. Você pode ver a lista de vulnerabilidades de software a qualquer momento. Os metadados das atualizações de software são baixados automaticamente no repositório do Servidor de Administração e nos repositórios dos pontos de distribuição como resultado da execução da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*. É possível criar essa tarefa pelo Assistente de Início Rápido do Kaspersky Security Center Cloud Console ou manualmente.

As atualizações de software para corrigir vulnerabilidades podem ser representadas como pacotes ou patches de distribuição completos. As atualizações de software que corrigem vulnerabilidades de software são denominadas *correções*. No Kaspersky Security Center Cloud Console, é possível corrigir as vulnerabilidades usando *correções recomendadas*. As correções recomendadas são as atualizações de software recomendadas para instalação pelos especialistas da Kaspersky.

Dependendo do modo Kaspersky Security Center Cloud Console e da licença atual, você pode usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades* para corrigir vulnerabilidades de software.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* corrige automaticamente várias vulnerabilidades, ao instalar as correções recomendadas. Para esta tarefa, você pode configurar manualmente certas regras para corrigir várias vulnerabilidades.

Por meio da tarefa *Corrigir vulnerabilidades* você pode corrigir vulnerabilidades ao instalar correções recomendadas para softwares da Microsoft.

Por motivos de segurança, todas as atualizações de software de terceiros que você instala usando o recurso Gerenciamento de Patches e Vulnerabilidades são verificadas automaticamente em busca de malwares pelas tecnologias da Kaspersky. Essas tecnologias são usadas para verificação automática de arquivos e incluem verificação de vírus, análise estática, análise dinâmica, análise de comportamento no ambiente sandbox e aprendizado de máquina.

Os especialistas da Kaspersky não realizam análises manuais de atualizações de softwares de terceiros que podem ser instaladas usando o recurso Gerenciamento de patches e vulnerabilidades. Além disso, os especialistas da Kaspersky não pesquisam vulnerabilidades (conhecidas ou desconhecidas) ou recursos não documentados nessas atualizações, nem realizam outros tipos de análise das atualizações além dos especificados no parágrafo acima.

As tarefas de instalação da atualização de software têm uma série de limitações. Essas limitações dependem da licença sob a qual você está usando o Kaspersky Security Center Cloud Console e do modo em que o Kaspersky Security Center Cloud Console está operando.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Para corrigir algumas vulnerabilidades de software, é necessário aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software, se o aceite do EULA for solicitado. Se você recusar o EULA, a vulnerabilidade do software não poderá ser corrigida.

As informações sobre cada vulnerabilidade corrigida são armazenadas no Servidor de Administração por 90 dias. Após esse tempo, são excluídas automaticamente.

Corrigir vulnerabilidades de software

Depois de obter a lista de vulnerabilidades de software, você pode corrigir as vulnerabilidades de software nos dispositivos gerenciados que executam o Windows. É possível corrigir vulnerabilidades de software no sistema operacional e em softwares de terceiros, incluindo softwares da Microsoft, criando e executando a tarefa *Corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

As tarefas de instalação da atualização de software têm uma série de limitações. Essas limitações dependem da licença sob a qual você está usando o Kaspersky Security Center Cloud Console e do modo em que o Kaspersky Security Center Cloud Console está operando.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Como opção, é possível criar uma tarefa para corrigir vulnerabilidades de software das seguintes maneiras:

- Abrindo a lista de vulnerabilidades e especificando quais vulnerabilidades corrigir.

  Como resultado, é criada uma nova tarefa para corrigir vulnerabilidades de software. Como opção, você pode adicionar as vulnerabilidades selecionadas a uma tarefa existente.

- Executando o assistente para Correção de vulnerabilidades.

  A disponibilidade deste recurso depende do modo do Kaspersky Security Center Cloud Console e da licença atual.

  O assistente simplifica a criação e a configuração de uma tarefa de correção de vulnerabilidades e permite eliminar a criação de tarefas redundantes que contenham as mesmas atualizações a serem instaladas.

Corrigindo vulnerabilidades de software usando a lista de vulnerabilidades

Para corrigir vulnerabilidades de software:

1. Abra uma das listas de vulnerabilidades:

   - Para abrir a lista geral de vulnerabilidades, No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   - Para abrir a lista de vulnerabilidades de um dispositivo gerenciado, no menu principal, acesse **Ativos (dispositivos) → Dispositivos gerenciados → <nome do dispositivo> → Avançado → Vulnerabilidades de software**.

   - Para abrir a lista de vulnerabilidades de um aplicativo específico, no meu principal, acesse **Operações → Aplicativos de terceiros → Registro de aplicativos → <nome do aplicativo> → Vulnerabilidades**.

   Uma página com uma lista de vulnerabilidades em softwares de terceiros é exibida.

2. Selecione uma ou mais vulnerabilidades na lista e clique no botão **Corrigir vulnerabilidade**.

Se a atualização de software recomendada para corrigir uma das vulnerabilidades selecionadas estiver ausente, uma mensagem informativa será exibida.

Para corrigir algumas vulnerabilidades de software, é necessário aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software, se o aceite do EULA for solicitado. Se você recusar o EULA, a vulnerabilidade do software não será corrigida.

3. Selecione uma das seguintes opções:

   - **Nova tarefa**

     O Assistente para nova tarefa inicia. Dependendo do modo do Kaspersky Security Center Cloud Console e de sua licença atual, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou tarefa *Corrigir vulnerabilidades* é pré-selecionada. Seguem abaixo as etapas do assistente para concluir a criação da tarefa.

   - **Corrigir vulnerabilidade (adicionar a regra à tarefa especificada)**

     Selecione uma tarefa à qual deseja adicionar as vulnerabilidades selecionadas. Dependendo do modo do Kaspersky Security Center Cloud Console e da licença atual, selecione a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*. Se você selecionar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, uma nova regra para corrigir as vulnerabilidades selecionadas será adicionada automaticamente à tarefa escolhida. Se você selecionar a tarefa *Corrigir vulnerabilidades*, as vulnerabilidades selecionadas serão adicionadas às propriedades da tarefa.

     A janela de propriedades da tarefa é aberta. Clique no botão **Salvar** para salvar as alterações.

Se você escolheu criar uma nova tarefa, a tarefa será criada e exibida na lista de tarefas em **Ativos (dispositivos)** → **Tarefas**. Se você optou por adicionar as vulnerabilidades a uma tarefa existente, as vulnerabilidades serão salvas nas propriedades da tarefa.

Para corrigir as vulnerabilidades de software de terceiros, inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*. Se você criou a tarefa *Corrigir vulnerabilidades*, deve especificar manualmente as atualizações de software para corrigir as vulnerabilidades de software listadas nas configurações da tarefa.

Corrigir vulnerabilidades de software usando o assistente para Correção de vulnerabilidades

A disponibilidade do assistente para Correção de vulnerabilidades depende da licença utilizada e do modo de funcionamento do Kaspersky Security Center Cloud Console.

Para corrigir vulnerabilidades de software usando o assistente para Correção de vulnerabilidades:

1. No menu principal, acesse **Operações** → **Gerenciamento de patches** → **Vulnerabilidades de software**.

   Uma página com uma lista de vulnerabilidades em softwares de terceiros instalados em dispositivos gerenciados é exibida.

2. Marque a caixa de seleção ao lado da vulnerabilidade que deseja corrigir.

3. Clique no botão **Executar o assistente para correção de vulnerabilidades**.

   O assistente para Correção de vulnerabilidades é iniciado. A página **Selecionar tarefa de correção de vulnerabilidades** exibe a lista de todas as tarefas existentes dos seguintes tipos:

   - *Instalar as atualizações necessárias e corrigir vulnerabilidades*

- *Instalar as atualizações do Windows Update*
- *Corrigir vulnerabilidades*

Você não pode modificar os dois últimos tipos de tarefas para instalar novas atualizações. Para instalar novas atualizações, você só pode usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

4. Se desejar que o assistente exiba apenas as tarefas que corrigem a vulnerabilidade selecionada, ative a opção **Exibir apenas tarefas que corrigem esta vulnerabilidade**.

5. Selecione o que deseja fazer:

   - Para iniciar uma tarefa, marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Iniciar**.
   - Para adicionar uma nova regra a uma tarefa existente:

     a. Marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Adicionar regra**.

     b. Na página aberta, configure a nova regra:

     - Regra para corrigir vulnerabilidades deste nível de gravidade

       Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

       Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

       Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

       Por padrão, esta opção está desativada.

     - **Regra para corrigir vulnerabilidades por meio de atualizações do mesmo tipo que a atualização definida como recomendada para a vulnerabilidade selecionada** (disponível apenas para vulnerabilidades de software da Microsoft)
     - **Regra para corrigir vulnerabilidades em aplicativos por fornecedor selecionado** (disponível apenas para vulnerabilidades de software de terceiros)
     - **Regra para corrigir uma vulnerabilidade em todas as versões do aplicativo selecionado** (disponível apenas para vulnerabilidades de software de terceiros)
     - **Regra para corrigir a vulnerabilidade selecionada**
     - Aprovar as atualizações que corrigem esta vulnerabilidade

       A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

       Por padrão, esta opção está desativada.

     c. Clique no botão **Adicionar**.

- Para criar uma tarefa:

  a. Clique no botão **Nova tarefa**.

  b. Na página aberta, configure a nova regra:

  - Regra para corrigir vulnerabilidades deste nível de gravidade

    Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

    Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

    Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

    Por padrão, esta opção está desativada.

  - **Regra para corrigir vulnerabilidades usando atualizações do tipo** (disponível apenas para vulnerabilidades de software da Microsoft)

  - **Regra para corrigir vulnerabilidades em aplicativos por fornecedor selecionado** (disponível apenas para vulnerabilidades de software de terceiros)

  - **Regra para corrigir uma vulnerabilidade em todas as versões do aplicativo selecionado** (disponível apenas para vulnerabilidades de software de terceiros)

  - **Regra para corrigir a vulnerabilidade selecionada**

  - Aprovar as atualizações que corrigem esta vulnerabilidade

    A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

    Por padrão, esta opção está desativada.

  c. Clique no botão **Adicionar**.

Se você optou por iniciar uma tarefa, poderá fechar o assistente. A tarefa será concluída no modo de segundo plano. Nenhuma outra ação será necessária.

Se você escolheu adicionar uma regra a uma tarefa existente, a janela de propriedades da tarefa é aberta. A nova regra já foi adicionada às propriedades da tarefa. Você pode visualizar ou modificar a regra ou outras configurações de tarefa. Clique no botão **Salvar** para salvar as alterações.

Caso tenha optado por criar uma tarefa, continue a criar a tarefa no assistente para Novas tarefas. A nova regra adicionada no assistente para Correção de vulnerabilidades é exibida no assistente para Novas tarefas. Ao concluir o assistente para Novas tarefas, a tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades* é adicionada à lista de tarefas.

Criar a tarefa Corrigir vulnerabilidades

A tarefa *Corrigir vulnerabilidades* permite corrigir vulnerabilidades de software em dispositivos gerenciados executando Windows.

A disponibilidade deste recurso depende do modo do Kaspersky Security Center Cloud Console e da licença atual. Recomendamos usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* em vez da tarefa *Corrigir vulnerabilidades*. A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* permite instalar várias atualizações e corrigir várias vulnerabilidades automaticamente, de acordo com as regras definidas por você.

As tarefas de instalação da atualização de software têm uma série de limitações. Essas limitações dependem da licença sob a qual você está usando o Kaspersky Security Center Cloud Console e do modo em que o Kaspersky Security Center Cloud Console está operando.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Para criar uma tarefa Corrigir vulnerabilidades:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Para o aplicativo Kaspersky Security Center Cloud Console, selecione o tipo de tarefa **Corrigir vulnerabilidades**.
4. Especifique o nome da tarefa que está criando.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.
6. Clique no botão **Adicionar**.

   A lista de vulnerabilidades é aberta.
7. Selecione as vulnerabilidades que deseja corrigir e, a seguir, clique em **OK**.
8. Especifique as configurações para reiniciar o sistema operacional:

   - **Não reiniciar o dispositivo**

     Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

   - **Reiniciar o dispositivo**

Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

  A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

  Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

  Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

  Por padrão, esta opção está desativada.

9. Especificar as configurações da conta:

- **Conta padrão**

  A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

  Por padrão, esta opção está selecionada.

- **Especificar conta**

  Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

- **Conta**

  Conta sob a qual a tarefa é executada.

- **Senha**

  Senha da conta sob a qual a tarefa será executada.

10. Se na página **Concluir a criação da tarefa**, você ativar a opção **Abrir detalhes da tarefa quando a criação for concluída**, você pode modificar as configurações padrão da tarefa. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

11. Clique no botão **Concluir**.

    A tarefa é criada e exibida na lista de tarefas.

12. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

13. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

14. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Criar a tarefa Instalar atualizações necessárias e corrigir vulnerabilidades

A disponibilidade da tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* depende do modo Kaspersky Security Center Cloud Console e da licença atual.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa permite instalar várias atualizações e corrigir várias vulnerabilidades, de acordo com determinadas regras.

Para instalar atualizações ou corrigir vulnerabilidades usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, execute uma das seguintes ações:

- Execute o assistente de Instalação das atualizações ou o assistente para Correção de vulnerabilidades.
- Crie uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.
- Adicione uma regra para instalação da atualização a uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.

As tarefas de instalação da atualização de software têm uma série de limitações. Essas limitações dependem da licença sob a qual você está usando o Kaspersky Security Center Cloud Console e do modo em que o Kaspersky Security Center Cloud Console está operando.

Para criar uma tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center Cloud Console, selecione o tipo de tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades**.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.
6. Especifique as regras para instalação da atualização e, então, especifique as seguintes configurações:

   - **Iniciar a instalação ao reiniciar ou fechar o dispositivo**

     Se esta opção estiver ativada, as atualizações serão instaladas quando o dispositivo for reiniciado ou desligado. Caso contrário, as atualizações são instaladas segundo o agendamento.

     Use esta opção caso a instalação das atualizações afete o desempenho do dispositivo.

     Por padrão, esta opção está desativada.

   - **Instalar os componentes gerais do sistema necessários**

     Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional

     Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

     Por padrão, esta opção está desativada.

   - **Permitir a instalação de novas versões dos aplicativos durante atualizações**

     Se esta opção estiver ativada, as atualizações serão permitidas quando resultarem na instalação de uma nova versão de um aplicativo de software.

     Se esta opção estiver desativada, o software não será atualizado. Você poderá então instalar novas versões do software manualmente ou através de outra tarefa. Por exemplo, você pode usar esta opção se a infraestrutura da sua empresa não tiver como base uma nova versão do software ou se você quiser verificar uma atualização usando uma infraestrutura de teste.

     Por padrão, esta opção está ativada.

     A atualização de um aplicativo pode causar o funcionamento incorreto de aplicativos dependentes instalados em dispositivos cliente.

   - **Baixar atualizações para o dispositivo sem instalá-las**

Se esta opção estiver ativada, o aplicativo baixa as atualizações em um dispositivo cliente, mas não as instala automaticamente. Você então poderá instalar manualmente as atualizações baixadas.

As atualizações da Microsoft são baixadas no armazenamento de sistema do Windows. Atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencentes à Kaspersky e à Microsoft) são baixados na pasta especificada no campo **Baixar atualizações para**.

Se esta opção estiver desativada, as atualizações serão instaladas no dispositivo automaticamente.

Por padrão, esta opção está desativada.

- **Pasta para download de atualizações**

  Esta pasta é usada para baixar atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft).

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará rastreamentos, mesmo se o rastreamento estiver desativado para o Agente de Rede no Utilitário de diagnóstico remoto do Kaspersky Security Center Cloud Console. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a gravar neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se este recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center Cloud Console. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

7. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Tempo de espera antes do fechamento forçado de aplicativos nas sessões bloqueadas (min)**

  Os aplicativos são fechados no modo forçado quando o dispositivo for bloqueado (automaticamente, após um intervalo especificado de inatividade ou manualmente).

  Se esta opção estiver ativada, os aplicativos serão forçados a fechar no dispositivo bloqueado após a expiração do intervalo de tempo especificado no campo de entrada.

  Se essa opção estiver ativada, os aplicativos não serão fechados no dispositivo bloqueado.

  Por padrão, esta opção está desativada.

8. Se na página **Concluir a criação da tarefa**, você ativar a opção **Abrir detalhes da tarefa quando a criação for concluída**, você pode modificar as configurações padrão da tarefa. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.

10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

11. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

12. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

Se os resultados da tarefa contiverem um aviso do erro 0x80240033 "Erro de atualização do Windows Update Agent 80240033 ("Não foi possível baixar os termos da licença.")", você poderá resolver esse problema no Registro do Windows.

Adicionar regras para instalação da atualização

A disponibilidade deste recurso depende do modo do Kaspersky Security Center Cloud Console e da licença atual.

Ao instalar atualizações de software ou corrigir vulnerabilidades de software usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é necessário especificar regras para a instalação da atualização. Essas regras determinam as atualizações a serem instaladas e as vulnerabilidades a serem corrigidas.

As configurações exatas dependem de você ter adicionado uma regra para todas as atualizações, para atualizações do Windows Update ou para atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software que não sejam a Kaspersky ou a Microsoft). Ao adicionar uma regra para atualizações do Windows Update ou atualizações de aplicativos de terceiros, é possível selecionar aplicativos e versões de aplicativo específicos para os quais deseja instalar atualizações. Ao adicionar uma regra para todas as atualizações, é possível selecionar atualizações específicas que deseja instalar e vulnerabilidades que deseja corrigir com a instalação das atualizações.

É possível adicionar uma regra para a instalação da atualização das seguintes maneiras:

- Adicionando uma regra ao criar uma nova tarefa do tipo Instalar as atualizações necessárias e corrigir vulnerabilidades.
- Adicionando uma regra na guia **Configurações do aplicativo** na janela de propriedades de uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.
- Por meio do assistente de Instalação das atualizações ou do assistente para Correção de vulnerabilidades.

Para adicionar uma nova regra para todas as atualizações:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para todas as atualizações**.

3. Na página **Critérios gerais**, use as listas suspensas para especificar as seguintes configurações:

   - **Conjunto de atualizações a instalar**

Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

- **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
- **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
- **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

- Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

  Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

  Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

  Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

  Por padrão, esta opção está desativada.

4. Na página **Atualizações**, selecione as atualizações a serem instaladas:

- Instalar todas as atualizações adequadas

  Instale todas as atualizações de software que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- Instalar apenas as atualizações da lista

  Instale somente as atualizações de software que você seleciona manualmente da lista. Essa lista contém todas as atualizações de software disponíveis.

  Por exemplo, pode ser necessário selecionar atualizações específicas nos seguintes casos: para verificar a instalação em um ambiente de teste, para atualizar somente aplicativos críticos ou para atualizar somente aplicativos específicos.

- Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas

Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

Por padrão, esta opção está ativada.

5. Na página **Vulnerabilidades**, selecione as vulnerabilidades que serão corrigidas instalando as atualizações selecionadas:

   - **Corrigir todas as vulnerabilidades que correspondem a outros critérios**

     Corrija todas as vulnerabilidades que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

   - **Corrigir somente vulnerabilidades da lista**

     Corrija somente as vulnerabilidades que você seleciona manualmente da lista. Essa lista contém todas as vulnerabilidades detectadas.

     Por exemplo, pode ser necessário selecionar vulnerabilidades específicas nos seguintes casos: para verificar a correção em um ambiente de teste, para corrigir vulnerabilidades somente em aplicativos críticos ou para corrigir vulnerabilidades somente em aplicativos específicos.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Para adicionar uma nova regra para atualizações do Windows Update:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para o Windows Update**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - **Conjunto de atualizações a instalar**

Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

- **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
- **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
- **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

- Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

  Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

  Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

  Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

  Por padrão, esta opção está desativada.

- Corrigir vulnerabilidades com um nível de gravidade do MSRC igual ou maior do que

  Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

  Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

  Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

  Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Categorias de atualizações**, selecione as categorias das atualizações a serem instaladas. Essas categorias são iguais às no Catálogo do Microsoft Update. Por padrão, todas as categorias estão selecionadas.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Para adicionar uma nova regra para as atualizações de aplicativos de terceiros:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para atualizações de terceiros**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção Configurações da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Visualizar informações sobre vulnerabilidades de software detectadas em todos os dispositivos gerenciados

Depois de verificar o software em dispositivos gerenciados quanto a vulnerabilidades, você pode visualizar a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados.

Para exibir a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados,

No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

A página exibe a lista de vulnerabilidades de software detectadas nos dispositivos cliente.

Você também pode gerar e visualizar o Relatório de vulnerabilidades.

Você pode especificar um filtro para visualizar a lista de vulnerabilidades de software. Clique no ícone **Filtro** ( ) no canto superior direito da lista de vulnerabilidades de software para gerenciar o filtro. Você também pode selecionar um dos filtros predefinidos na lista suspensa **Filtros predefinidos** acima da lista de vulnerabilidades de software.

Você pode obter informações detalhadas sobre qualquer vulnerabilidade na lista.

Para obter informações sobre uma vulnerabilidade de software:

Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade.

A janela de propriedades da vulnerabilidade de software é aberta.

Visualizar informações sobre vulnerabilidades de software detectadas no dispositivo gerenciado selecionado

Você pode visualizar informações sobre vulnerabilidades de software detectadas no dispositivo gerenciado selecionado que executa o Windows.

Para exportar a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Ativos (dispositivos) → Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo para o qual você deseja visualizar as vulnerabilidades de software detectadas.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Na janela de propriedades do dispositivo selecionado selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Vulnerabilidades de software**.

   A lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado é exibida.

Para visualizar as propriedades da vulnerabilidade de software selecionada,

Clique no link com o nome da vulnerabilidade de software na lista de vulnerabilidades de software.

A janela de propriedades de vulnerabilidade de software selecionada é exibida.

Visualizar as estatísticas de vulnerabilidades em dispositivos gerenciados

Você pode visualizar estatísticas para cada vulnerabilidade de software em dispositivos gerenciados. As estatísticas são representadas como um diagrama. O diagrama exibe o número de dispositivos com os seguintes status:

- *Ignorado em: <número de dispositivos>*. O status será atribuído se, nas propriedades da vulnerabilidade, o usuário tiver definido manualmente a opção para ignorá-la.
- *Corrigido em: <número de dispositivos>*. O status será atribuído se a tarefa para correção de vulnerabilidade for concluída com êxito.
- *Correção agendada em: <número de dispositivos>*. O status será atribuído se o usuário tiver criado a tarefa para correção de vulnerabilidades, mas a tarefa ainda não tiver sido executada.
- *Correção aplicada em: <número de dispositivos>*. O status será atribuído se o usuário tiver selecionado manualmente uma atualização de software para correção de vulnerabilidades, mas essa atualização de software não tiver corrigido a vulnerabilidade.
- *Correção necessária em: <número de dispositivos>*. Esse status é atribuído se a vulnerabilidade tiver sido corrigida somente em alguns dispositivos gerenciados e precisar ser corrigida em mais dispositivos gerenciados.

Para exibir as estatísticas de uma vulnerabilidade nos dispositivos gerenciados:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   A página exibe uma lista de vulnerabilidades nos aplicativos detectados nos dispositivos gerenciados.

2. Selecione a caixa de seleção ao lado da vulnerabilidade necessária.

3. Clique no botão **Estatísticas de vulnerabilidades em dispositivos**.

   O diagrama dos status de vulnerabilidade é exibido. Clicar em um status abre uma lista de dispositivos nos quais a vulnerabilidade tem o status selecionado.

Exportar a lista de vulnerabilidades de software para um arquivo

Você pode exportar a lista de vulnerabilidades exibidas para os arquivos CSV ou TXT. Você pode usar esses arquivos, por exemplo, para enviá-los ao seu gerente de segurança de informações ou para armazená-los para fins de estatística.

Para exportar a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados para um arquivo de texto:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   A página exibe uma lista de vulnerabilidades nos aplicativos detectados nos dispositivos gerenciados.

2. Clique no botão **Exportar para TXT** ou **Exportar para CSV**, dependendo do formato de exportação preferido.

   O arquivo que contém a lista de vulnerabilidades de software é baixado no dispositivo que você está usando no momento.

Para exportar a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado para um arquivo de texto:

1. Abra a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado.

2. Selecione as vulnerabilidades de software que você deseja exportar.

   Pule esta etapa se desejar exportar uma lista completa de vulnerabilidades de software detectadas no dispositivo gerenciado.

   Se você deseja exportar a lista completa de vulnerabilidades de software detectadas no dispositivo gerenciado, apenas as vulnerabilidades exibidas na página atual serão exportadas.

3. Clique no botão **Exportar para TXT** ou **Exportar para CSV**, dependendo do formato de exportação preferido.

O arquivo que contém a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado é baixado no dispositivo que você está usando no momento.

Ignorar as vulnerabilidades de software

Você pode ignorar as vulnerabilidades do software a ser corrigidas. Os motivos para ignorar vulnerabilidades de software, por exemplo, os seguintes:

- A vulnerabilidade de software não é considerada crítica para sua organização.
- Você entende que a correção de vulnerabilidade do software pode danificar os dados relacionados ao software que exigia a correção da vulnerabilidade.
- Você tem certeza de que a vulnerabilidade do software não é perigosa para a rede da sua organização porque usa outras medidas para proteger seus dispositivos gerenciados.

Você pode ignorar uma vulnerabilidade de software em todos os dispositivos gerenciados ou apenas nos dispositivos gerenciados selecionados.

Para ignorar uma vulnerabilidade de software em todos os dispositivos gerenciados:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   A página exibe a lista de vulnerabilidades de software detectadas nos dispositivos gerenciados.

2. Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade de software que você deseja ignorar.

   A janela Propriedades de vulnerabilidade do software é aberta.

3. Na guia **Geral**, ative a opção **Ignorar vulnerabilidade**.

4. Clique no botão **Salvar**.

   A janela de propriedades de vulnerabilidade do software é fechada.

A vulnerabilidade de software é ignorada em todos os dispositivos gerenciados.

Para ignorar uma vulnerabilidade de software no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Ativos (dispositivos) → Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo no qual você deseja ignorar uma vulnerabilidade de software.

   A janela Propriedades do dispositivo é aberta.

3. Na janela Propriedades do dispositivo, selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Vulnerabilidades de software**.

   A lista de vulnerabilidades de software detectadas no dispositivo é exibida.

5. Na lista de vulnerabilidades de software, selecione a vulnerabilidade que você deseja ignorar no dispositivo selecionado.

   A janela Propriedades de vulnerabilidade do software é aberta.

6. Na janela de propriedades da vulnerabilidade de software, na guia **Geral**, ative a opção **Ignorar vulnerabilidade**.

7. Clique no botão **Salvar**.

   A janela de propriedades de vulnerabilidade do software é fechada.

8. Feche a janela Propriedades do dispositivo.

A vulnerabilidade de software é ignorada no dispositivo selecionado.

A vulnerabilidade de software ignorada não será corrigida após a conclusão das tarefas *Corrigir vulnerabilidades* ou *Instalar as atualizações necessárias e corrigir vulnerabilidades*. É possível excluir as vulnerabilidades de software ignoradas na lista de vulnerabilidades por meio do filtro.

Definindo o período máximo de armazenamento para as informações sobre vulnerabilidades corrigidas

Para definir o período máximo de armazenamento no banco de dados para as informações sobre as vulnerabilidades que já foram corrigidas em dispositivos gerenciados:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na página exibida, prossiga para a guia **Repositório de eventos**.

3. Especifique o período máximo de armazenamento para as informações sobre vulnerabilidades corrigidas no banco de dados.

   Por padrão, o período de armazenamento é de 7 dias no modo de avaliação e 60 dias no modo comercial. O limite máximo é de 14 dias no modo de avaliação e 365 dias no modo comercial.

4. Clique em **Salvar**.

O período máximo de armazenamento para as informações sobre as vulnerabilidades corrigidas é limitado ao número especificado de dias.

Gerenciando a execução de aplicativos em dispositivos cliente

Esta seção descreve os recursos do Kaspersky Security Center Cloud Console relacionados ao gerenciamento de aplicativos executados nos dispositivos cliente.

Cenário: Gerenciamento de Aplicativos

Você pode gerenciar a inicialização de aplicativos nos dispositivos cliente. Você pode permitir ou bloquear a execução de aplicativos em dispositivos gerenciados. Essa funcionalidade é realizada pelo componente Controle de Aplicativos. Você pode gerenciar aplicativos instalados em dispositivos Windows ou Linux.

Para sistemas operacionais baseados em Linux, o componente Controle de Aplicativos está disponível a partir do Kaspersky Endpoint Security 11.2 for Linux.

Pré-requisitos

- O Kaspersky Security Center Cloud Console está implementado em sua organização.
- A política do Kaspersky Endpoint Security for Windows ou do Kaspersky Endpoint Security for Linux está criada e ativa.

Fases

O cenário de uso do Controle de Aplicativos prossegue em fases:

1. **Formar e visualizar a lista de aplicativos em dispositivos cliente**

   Esta etapa ajuda a descobrir quais aplicativos estão instalados nos dispositivos gerenciados. Você pode exibir a lista de aplicativos e decidir quais aplicativos deseja permitir e quais deseja proibir, de acordo com as políticas de segurança de sua organização. As restrições podem estar relacionadas às políticas de segurança da informação em sua organização. Você pode pular esta fase se souber exatamente quais aplicativos estão instalados nos dispositivos gerenciados.

   Instruções de como proceder: Obter e visualizar uma lista instalados nos dispositivos cliente

2. **Formar e visualizar a lista de arquivos executáveis em dispositivos cliente**

   Esta etapa ajuda a descobrir quais arquivos executáveis são encontrados nos dispositivos gerenciados. Exiba a lista de arquivos executáveis e compare-a com a lista de arquivos executáveis permitidos e proibidos. As restrições sobre a utilização de arquivos executáveis podem estar relacionadas às políticas de segurança da informação em sua organização. Você pode pular esta fase se souber exatamente quais arquivos executáveis estão instalados nos dispositivos gerenciados.

   Instruções de como proceder: Obter e visualizar uma lista de arquivos executáveis instalados em dispositivos cliente

3. **Criar categorias de aplicativo para os aplicativos usados na sua organização**

   Analise a lista de aplicativos e arquivos executáveis armazenados nos dispositivos gerenciados. Baseando-se na análise, crie categorias de aplicativo. É recomendável criar uma categoria "Aplicativos de trabalho" que cubra o conjunto padrão de aplicativos usados na sua organização. Se diferentes grupos de segurança usarem conjuntos diferentes de aplicativos em seu trabalho, uma categoria de aplicativo poderá ser criada para cada grupo de segurança.

   Dependendo do conjunto de critérios para criar uma categoria de aplicativos, você pode criar categorias de aplicativos de dois tipos.

Instruções de como proceder: Criar categoria de aplicativos com conteúdo adicionado manualmente, Criar categoria de aplicativos que inclua arquivos executáveis de dispositivos selecionados

4. **Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows**

   Configure o componente Controle de Aplicativos na política do Kaspersky Endpoint Security for Windows usando as categorias de aplicativos criadas na fase anterior.

   Instruções de como proceder: Configurar o Controle de Aplicativos na política do Kaspersky Endpoint Security for Windows

5. **Ativar o componente Controle de Aplicativos no modo de teste**

   Para garantir que as regras do Controle de Aplicativos não bloqueiem os aplicativos necessários para o trabalho do usuário, é recomendável ativar o teste das regras do Controle de Aplicativos e analisar a sua operação após a criação de novas regras. Quando o teste está ativado, o Kaspersky Endpoint Security for Windows não bloqueia os aplicativos cuja inicialização é proibida pelas regras do Controle de Aplicativos, mas envia notificações sobre a inicialização ao Servidor de Administração.

   Ao testar as regras do Controle de Aplicativos, é recomendável realizar as seguintes ações:

   - Determine o período de teste. O período de teste pode variar de vários dias a dois meses.
   - Examine os eventos resultantes do teste da operação do Controle de Aplicativos.

   Instruções de como proceder: Configurar o componente Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows. Siga estas instruções e ative o modo de teste no processo de configuração.

6. **Alterar as configurações das categorias de aplicativos do componente Controle de Aplicativos**

   Se necessário, faça alterações nas configurações do Controle de Aplicativos. Com base nos resultados do teste, você pode adicionar arquivos executáveis relativos a eventos do componente Controle de Aplicativos a uma categoria de aplicativo com conteúdo adicionado manualmente.

   Instruções de como proceder: Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos

7. **Aplicar as regras do Controle de Aplicativos no modo de operação**

   Após as regras de Controle de Aplicativos terem sido testadas e a configuração das categorias de aplicativo estar concluída, você pode aplicar as regras do Controle de Aplicativos no modo de operação.

   Instruções de como proceder: Configurar o componente Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows. Siga estas instruções e desative o modo de teste no processo de configuração.

8. **Verificar a configuração do Controle de Aplicativos**

   Certifique-se do seguinte:

   - A lista de categorias de aplicativos não está vazia. Veja a lista de categorias de aplicativos e verifique se ela contém as categorias que você configurou.
   - O Controle de Aplicativos é configurado usando categorias de aplicativos criadas. Veja as configurações da política do Kaspersky Endpoint Security for Windows e certifique-se de que o Controle de Aplicativos foi configurado em **Configurações do aplicativo** → **Controles de segurança** → **Controle de Aplicativos**.
   - As regras do Controle de Aplicativos são aplicadas no modo de operação. Verifique o modo na política do Kaspersky Endpoint Security for Windows e certifique-se de ter desativado o **Modo de teste** em **Configurações do aplicativo** → **Controles de Segurança** → **Controle de Aplicativos**.

Resultados

Quando o cenário estiver concluído, a inicialização dos aplicativos nos dispositivos gerenciados será controlada. Os usuários podem iniciar apenas os aplicativos permitidos na sua organização e não podem iniciar aplicativos proibidos na sua organização.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux

Sobre o Controle de Aplicativos

O componente Controle de Aplicativos monitora as tentativas do usuário para iniciar aplicativos e regula a inicialização de aplicativos usando as regras do Controle de Aplicativos.

O componente Controle de Aplicativos está disponível para Kaspersky Endpoint Security for Windows e para Kaspersky Endpoint Security for Linux (versão 11.2 ou posterior). Todas as instruções nesta seção descrevem a configuração do Controle de Aplicativos para o Kaspersky Endpoint Security.

A inicialização de aplicativos cujas configurações não correspondem a nenhuma das regras do Controle de Aplicativos é regulada pelo modo de operação selecionado do componente:

- *Lista de bloqueio*. O modo é usado se você deseja permitir a inicialização de todos os aplicativos, exceto os aplicativos especificados nas regras de bloqueio. O modo *Lista de bloqueio* é selecionado por padrão.
- *Lista de permissão*. O modo é usado se você deseja bloquear a inicialização de todos os aplicativos, exceto os aplicativos especificados nas regras de permissão.

As regras de controle de aplicativos são implementadas por meio de categorias de aplicativos. Você cria categorias de aplicativos definindo critérios específicos. No Kaspersky Security Center Cloud Console, existem dois tipos de categorias de aplicativos:

- Categoria com conteúdo adicionado manualmente. Você define condições, por exemplo, metadados do arquivo, código de hash do arquivo, certificado do arquivo, categoria KL, caminho do arquivo, para incluir arquivos executáveis na categoria.
- Categoria que inclui os arquivos executáveis dos dispositivos selecionados. Você especifica um dispositivo cujos arquivos executáveis são incluídos automaticamente na categoria.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux

Obter e visualizar uma lista de aplicativos instalados nos dispositivos cliente

O Kaspersky Security Center Cloud Console executa um inventário de todos os softwares instalados nos dispositivos cliente gerenciados que executam o Linux e Windows.

O Agente de Rede compila uma lista de aplicativos instalados em um dispositivo cliente e, a seguir, transmite esta lista para o Servidor de Administração. São necessários cerca de 10 a 15 minutos para o Agente de Rede atualizar a lista de aplicativos.

Para dispositivos cliente baseados no Windows, o Agente de Rede recebe a maioria das informações sobre os aplicativos instalados do registro do Windows. Para dispositivos cliente baseados em Linux, os gerenciadores de pacotes fornecem ao Agente de Rede informações sobre os aplicativos instalados.

Para exibir a lista de aplicativos instalados nos dispositivos gerenciados:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos**.

   A página exibe uma tabela com os aplicativos instalados nos dispositivos gerenciados. Selecione o aplicativo para visualizar suas propriedades, por exemplo, nome do fornecedor, número da versão, lista de arquivos executáveis, lista de dispositivos nos quais o aplicativo está instalado, lista de atualizações de software disponíveis e lista de vulnerabilidades de software detectadas.

2. É possível agrupar e filtrar os dados da tabela com os aplicativos instalados da seguinte forma:

   - Clique no ícone de configurações ( ) no canto superior direito da tabela.

     No menu **Configurações de colunas** resultante, selecione as colunas a serem exibidas na tabela. Para visualizar o tipo de sistema operacional dos dispositivos clientes nos quais o aplicativo está instalado, selecione a coluna **Tipo de sistema operacional**.

   - Clique no ícone de filtro ( ) no canto superior direito da tabela e depois, especifique e aplique o critério de filtro no menu resultante.

     A tabela filtrada de aplicativos instalados é exibida.

Para visualizar a lista de aplicativos instalados em um dispositivo gerenciado específico,

No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados** → **<nome do dispositivo>** → **Avançado** → **Registro de aplicativos**. Neste menu, é possível exportar a lista de aplicativos para um arquivo CSV ou TXT.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux

Obter e visualizar uma lista de arquivos executáveis instalados em dispositivos clientes

Você pode obter uma lista de arquivos executáveis que estão instalados em dispositivos gerenciados. Para o inventário de arquivos executáveis, você deve criar uma tarefa de inventário.

O recurso de inventário de arquivos executáveis está disponível para os seguintes aplicativos:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux (versão 11.2 e posterior)

É possível reduzir a carga no banco de dados enquanto as informações sobre os aplicativos instalados são obtidas. Para fazer isso, recomendamos executar uma tarefa de inventário em dispositivos de referência nos quais um conjunto padrão de software está instalado.

Para criar uma tarefa de inventário para arquivos executáveis em dispositivos cliente:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.

   A lista de tarefas é exibida.

2. Clique no botão **Adicionar**.

   O Assistente para nova tarefa inicia. Siga as etapas do Assistente.

3. Na página **Nova tarefa**, na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Windows ou Kaspersky Endpoint Security for Linux, dependendo do tipo de sistema operacional dos dispositivos clientes.

4. Na lista suspensa **Tipo de tarefa**, selecione **Inventário**.

5. Na página **Concluir a criação da tarefa**, clique no botão **Concluir**.

   Após a conclusão do assistente para novas tarefas, a tarefa **Inventário** é criada e configurada. Se desejar, você pode alterar as configurações da tarefa criada. A tarefa recém-criada é exibida na lista de tarefas.

Para uma descrição detalhada da tarefa de inventário, consulte as seguintes ajudas:

- Ajuda do Kaspersky Endpoint Security for Windows
- Ajuda do Kaspersky Endpoint Security for Linux

Após a tarefa **Inventário** tiver sido executada, a lista de arquivos executáveis instalados nos dispositivos gerenciados é formada e você pode visualizá-la.

Durante o inventário, arquivos executáveis nos seguintes formatos são detectados: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Para exibir a lista dos arquivos executáveis armazenados nos dispositivos cliente,

No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Arquivos executáveis**.

A página exibe a lista de arquivos executáveis instalados nos dispositivos cliente.

Também é possível enviar o arquivo executável de um dispositivo gerenciado para a Kaspersky para verificar possíveis ameaças.

Para enviar o arquivo executável do dispositivo gerenciado para a Kaspersky:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Arquivos executáveis**.

2. Clique no link do arquivo executável que deseja enviar para a Kaspersky.

3. Na janela que é aberta, vá para a seção **Dispositivos** e marque a caixa de seleção do dispositivo gerenciado do qual você deseja enviar o arquivo executável.

Antes de enviar o arquivo executável, certifique-se de que o dispositivo gerenciado tenha uma conexão direta com o Servidor de Administração marcando a **caixa de seleção** Não desconectar do Servidor de Administração. O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

4. Clique no botão **Enviar à Kaspersky**.

O arquivo executável selecionado é baixado para envio posterior à Kaspersky.

Criar uma categoria de aplicativos com conteúdo adicionado manualmente

Você pode especificar um conjunto de critérios como um modelo de arquivos executáveis cuja inicialização deseja permitir ou bloquear na sua organização. Com base nos arquivos executáveis correspondentes aos critérios, você poderá criar uma categoria de aplicativos e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria de aplicativos com conteúdo adicionado manualmente:

1. No menu principal, acesse **Operações → Aplicativos de terceiros → Categorias de aplicativos**.

   A página com uma lista de categorias de aplicativos é exibida.

2. Clique no botão **Adicionar**.

   O Assistente para Novas Categorias inicia. Siga as etapas do Assistente.

3. Na página **Selecionar método de criação de categoria** do assistente, selecione a opção **Categoria com conteúdo adicionado manualmente. Os dados dos arquivos executáveis são adicionados manualmente à categoria**.

4. Na página **Condições** do assistente, clique no botão **Adicionar** para adicionar um critério condicional para a inclusão de arquivos na categoria sendo criada.

5. Na página **Critérios da condição**, selecione um tipo de regra para a criação de categoria na lista:

   - Da categoria KL

     Se esta opção estiver selecionada, você poderá especificar uma categoria de aplicativos da Kaspersky como a condição para adicionar aplicativos da categoria do usuário. Os aplicativos da categoria da Kaspersky especificada serão adicionados à categoria de aplicativos do usuário.

   - Selecionar certificado do repositório

     Se esta opção estiver selecionada, você pode especificar certificados do armazenamento. Arquivos executáveis que tenham sido assinados de acordo com os certificados especificados serão adicionados à categoria de usuário.

   - Especificar caminho para o aplicativo (máscaras aceitas)

     Se esta opção estiver selecionada, você poderá especificar o caminho para a pasta no dispositivo cliente contendo os arquivos executáveis a serem adicionados à categoria de aplicativos do usuário.

- Unidade removível

  Se esta opção estiver selecionada, você pode especificar o tipo de mídia (qualquer unidade ou unidade removível) no qual o aplicativo será executado. Os aplicativos que foram executados no tipo de unidade selecionado são adicionados à categoria de aplicativo do usuário.

- **Hash, metadados ou certificado**:

  - Selecionar na lista de arquivos executáveis

    Se esta opção estiver selecionada, você poderá utilizar a lista de arquivos executáveis no dispositivo cliente para selecionar e adicionar aplicativos deles à categoria.

  - Selecionar do registro de aplicativos

    Se esta opção for selecionada, o registro dos aplicativos será exibido. Você pode selecionar um aplicativo no registro e especificar os seguintes metadados do arquivo:

    - Nome do arquivo.
    - Versão do arquivo. Você pode especificar um valor preciso da versão ou descrever uma condição, por exemplo "posterior a 5.0".
    - Nome do aplicativo.
    - Versão do aplicativo. Você pode especificar um valor preciso da versão ou descrever uma condição, por exemplo "posterior a 5.0".
    - Fornecedor.

  - Especificar manualmente

Se esta opção estiver selecionada, você deve especificar hash do arquivo, metadados ou certificado como a condição para adicionar aplicativos à categoria do usuário.

Hash do arquivo

Dependendo da versão do aplicativo de segurança instalado em dispositivos na sua rede, você deve selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center Cloud Console de arquivos nesta categoria. As informações sobre os valores de hash calculado são armazenadas no banco de dados do Servidor de Administração. O armazenamento de valores hash não aumenta significativamente o tamanho do banco de dados.

SHA-256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores suportam o cálculo SHA-256. O cálculo da função MD5 hash é suportado por todas as versões anteriores do Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center Cloud Console de arquivos na categoria:

- Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem versões do Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posteriores, selecione a caixa de seleção **SHA-256**. Não recomendamos que você adicione nenhuma categoria criada de acordo com o critério do hash SHA-256 de um arquivo executável para versões anteriores à versão do Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Isto pode resultar em falhas na operação do aplicativo de segurança. Neste caso, você pode usar a função MD5 hash criptográfica para arquivos da categoria.

- Se alguma versão anterior ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows estiver instalada na sua rede, selecione **Hash MD5**. Você não pode adicionar uma categoria que foi criada com base no critério do checksum MD5 de um arquivo executável para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou versões posteriores. Neste caso, você pode usar a função SHA-256 hash criptográfica para arquivos da categoria.

- Se diferentes dispositivos usam versões anteriores e posteriores do Kaspersky Endpoint Security 10, selecione as caixas de seleção **SHA-256** e **Hash MD5**.

Metadados

Se esta opção for selecionada, você poderá especificar os metadados do arquivo como nome, versão e fornecedor. Os metadados serão enviados ao Servidor de Administração. Os arquivos executáveis que contenham os mesmos metadados serão adicionados à categoria de aplicativos.

Certificado

Se esta opção estiver selecionada, você pode especificar certificados do armazenamento. Arquivos executáveis que tenham sido assinados de acordo com os certificados especificados serão adicionados à categoria de usuário.

- Do arquivo ou do pacote MSI/pasta arquivada

Se esta opção estiver selecionada, você poderá especificar um arquivo de instalador MSI como a condição para adicionar aplicativos à categoria de usuário. Os metadados do instalador do aplicativo serão enviados ao Servidor de Administração. Os aplicativos para os quais o instalador de metadados for o mesmo para o instalador MSI especificado, são adicionados à categoria de aplicativos do usuário.

O critério selecionado é adicionado à lista de condições.

Você pode adicionar quantos critérios para a categoria de aplicativo de criação forem necessários.

6. Na página **Exclusões** do assistente, clique no botão **Adicionar** para adicionar um critério condicional exclusivo para excluir arquivos da categoria sendo criada.

7. Na página **Critérios da condição**, selecione um tipo de regra na lista tal como você selecionou um tipo de regra para a criação da categoria.

Quando o assistente for concluído, uma categoria de aplicativos será criada. Ela é exibida na lista de categorias de aplicativos. Você pode usar a categoria de aplicativos criada ao configurar o Controle de Aplicativos.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux

Criar a categoria de aplicativo que inclua arquivos executáveis dos dispositivos selecionados

Você pode usar arquivos executáveis de dispositivos selecionados como um modelo de arquivos executáveis que deseja permitir ou bloquear. Com base nos arquivos executáveis dos dispositivos selecionados, você pode criar uma categoria de aplicativo e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria de aplicativo que inclui arquivos executáveis de dispositivos selecionados:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Categorias de aplicativos**.

   A página com uma lista de categorias de aplicativos é exibida.

2. Clique no botão **Adicionar**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na página **Selecionar método de criação de categoria** do assistente, especifique o nome da categoria e selecione a opção **Categoria que inclui arquivos executáveis dos dispositivos selecionados. Esses arquivos executáveis são processados automaticamente e suas métricas são adicionadas à categoria**.

4. Clique em **Adicionar**.

5. Na janela que se abre, selecione um ou mais dispositivos cujos arquivos executáveis serão usados para criar a categoria de aplicativos.

6. Especificar as seguintes configurações:

   - **Algoritmo de cálculo do valor hash**

Dependendo da versão do aplicativo de segurança instalado em dispositivos na sua rede, você deve selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center Cloud Console de arquivos nesta categoria. As informações sobre os valores de hash calculado são armazenadas no banco de dados do Servidor de Administração. O armazenamento de valores hash não aumenta significativamente o tamanho do banco de dados.

SHA-256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores suportam o cálculo SHA-256. O cálculo da função MD5 hash é suportado por todas as versões anteriores do Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center Cloud Console de arquivos na categoria:

- Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem versões do Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posteriores, selecione a caixa de seleção **SHA-256**. Não recomendamos que você adicione nenhuma categoria criada de acordo com o critério do hash SHA-256 de um arquivo executável para versões anteriores à versão do Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Isto pode resultar em falhas na operação do aplicativo de segurança. Neste caso, você pode usar a função MD5 hash criptográfica para arquivos da categoria.

- Se alguma versão anterior ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows estiver instalada na sua rede, selecione **Hash MD5**. Você não pode adicionar uma categoria que foi criada com base no critério do checksum MD5 de um arquivo executável para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou versões posteriores. Neste caso, você pode usar a função SHA-256 hash criptográfica para arquivos da categoria.

Se diferentes dispositivos usam versões anteriores e posteriores do Kaspersky Endpoint Security 10, selecione as caixas de seleção **SHA-256** e **Hash MD5**.

A caixa de seleção **Calcular o SHA-256 para arquivos nessa categoria (suportado pelo Kaspersky Endpoint Security 10 Service Pack 2 for Windows e quaisquer versões posteriores)** é selecionada por padrão.

A caixa de seleção **Calcular o MD5 para os arquivos nesta categoria (suportado pelas versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** é selecionado por padrão.

- Sincronizar dados com o repositório do Servidor de Administração

Selecione esta opção se você desejar que o Servidor de Administração verifique periodicamente as alterações na pasta (ou pastas) especificada.

Por padrão, esta opção está desativada.

Se você ativar esta opção, especifique o período (em horas) para verificar as alterações nas pastas especificadas. Por padrão, o intervalo de verificação é de 24 horas.

- Tipo de arquivo

Nesta seção, você pode especificar o tipo de arquivo usado para criar a categoria de aplicativo.

Todos os arquivos. Todos os arquivos são levados em consideração durante a criação da categoria. Por padrão, esta opção está selecionada.

Somente arquivos fora das categorias de aplicativos. Somente arquivos fora das categorias de aplicativos são levados em consideração durante a criação da categoria.

- **Pastas**

  Nesta seção, você pode especificar quais pastas dos dispositivos selecionados contendo arquivos usados para criar a categoria de aplicativos.

  Todas as pastas. Todas as pastas são levadas em consideração para a categoria de criação. Por padrão, esta opção está selecionada.

  Pasta especificada. Somente a pasta especificada é levada em consideração para a categoria de criação. Se você selecionar esta opção, deverá especificar o caminho para a pasta.

Quando o assistente for concluído, uma categoria de aplicativos será criada. Ela é exibida na lista de categorias de aplicativos. Você pode usar a categoria de aplicativos criada ao configurar o Controle de Aplicativos.

Visualizando a lista de categorias de aplicativo

Você pode visualizar a lista de categorias de aplicativos configuradas e as configurações de cada uma delas.

Para visualizar a lista de categorias de aplicativos,

No menu principal, vá para **Operações → Aplicativos de terceiros → Categorias de aplicativos**.

A página com uma lista de categorias de aplicativos é exibida.

Para visualizar propriedades de uma categoria de aplicativos,

Clique no nome da categoria de aplicativos.

A janela de propriedades da categoria de aplicativos é exibida. As propriedades estão agrupadas em várias guias.

Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows

Após você criar as categorias do Controle de Aplicativos, poderá usá-las para configurar o Controle de Aplicativos nas políticas do Kaspersky Endpoint Security for Windows.

Para configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows:

1. No menu principal, vá para **Ativos (dispositivos) → Políticas e perfis**.

   Uma página com uma lista de políticas é exibida.

2. Clique em Política do **Kaspersky Endpoint Security for Windows**.

   A janela Propriedades da política será aberta.

3. Acesse **Configurações do aplicativo → Controles de Segurança → Controle de Aplicativos**.

   A janela **Controle de Aplicativos** com as configurações de Controle de Aplicativos é exibida.

4. A opção **Controle de Aplicativos** está ativada por padrão. Alterne o botão **Controle de aplicativos DESATIVADO** para desativar a opção.

5. No configurações de bloqueio **Configurações de Controle de Aplicativos**, ative o modo de operação para aplicar as Regras de Controle de Aplicativos e permita que o Kaspersky Endpoint Security for Windows bloqueie a inicialização de aplicativos.

   Se você quiser testar as Regras de Controle de Aplicativos, na seção **Configurações de Controle de Aplicativos**, ative o modo de teste. No modo de teste, o Kaspersky Endpoint Security for Windows não bloqueia a inicialização de aplicativos, mas registra no relatório informações sobre as regras acionadas. Clique no link **Ver relatório** para visualizar esta informação.

6. Ative a opção **Controlar carregamento dos módulos DLL** caso desejar que o Kaspersky Endpoint Security for Windows monitore o carregamento dos módulos DLL quando os aplicativos forem iniciados pelos usuários.

   As informações sobre o módulo e o aplicativo que carregou o módulo serão salvas em um relatório.

   O Kaspersky Endpoint Security for Windows monitora apenas os módulos DLL e drivers carregados após a opção **Controlar carregamento dos módulos DLL** tiver sido selecionada. Reinicie o computador após selecionar a opção **Controlar carregamento dos módulos DLL** caso desejar que o Kaspersky Endpoint Security for Windows monitore todos os módulos DLL e drivers, incluindo aqueles carregados antes do Kaspersky Endpoint Security for Windows ter sido iniciado.

7. (Opcional) No bloco **Modelos de mensagem**, altere o modelo da mensagem exibida quando um aplicativo é impedido de iniciar e o modelo da mensagem de e-mail enviada para você.

8. Nas configurações de bloqueio **Modo de Controle de Aplicativos**, selecione o modo **Lista de bloqueio** ou **Lista de permissão**.

   Por padrão, o modo **Lista de bloqueio** é selecionado.

9. Clique no link **Configurações das listas de regras**.

   A janela **Listas de bloqueio e permissão** é aberta para permitir a adição de uma categoria de aplicativo. Por padrão, a guia **Lista de bloqueio** é selecionada se o modo **Lista de bloqueio** estiver selecionado ou a guia **Lista de aprovação** é selecionada se o modo **Lista de aprovação** estiver selecionado.

10. Na janela **Listas de bloqueio e de aprovação**, clique no botão **Adicionar**.

    A janela **Regra de Controle de Aplicativos** abre.

11. Clique no link **Escolha uma categoria**.

    A janela **Categoria de Aplicativo** é aberta.

12. Adicione a categoria de aplicativo (ou categorias) que você criou anteriormente.

    Você pode editar as configurações de uma categoria criada clicando no botão **Editar**.

    Você pode criar uma nova categoria clicando no botão **Adicionar**.

    Você pode excluir uma categoria da lista clicando no botão **Excluir**.

13. Após lista de categorias de aplicativos estiver completa, clique no botão **OK**.

    A janela **Categoria de Aplicativos** é fechada.

14. Na janela Regra de **Controle de Aplicativos**, na seção **Pessoas e seus direitos**, crie uma lista de usuários e grupos de usuários para aplicar a regra de Controle de Aplicativos.

15. Clique no botão **OK** para salvar as configurações e fechar a janela **Regra de Controle de Aplicativos**.

16. Clique no botão **OK** para salvar as configurações e fechar a janela **Listas de bloqueio e de aprovação**.

17. Clique no botão **OK** para salvar as configurações e fechar a janela **Controle de Aplicativos**.

18. Feche a janela com as configurações da política do Kaspersky Endpoint Security for Windows.

    O Controle de Aplicativos está configurado. Após a política ter sido propagada para os dispositivos cliente, a inicialização dos arquivos executáveis é gerenciada.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux

Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos

Após configurar o Controle de Aplicativos nas políticas do Kaspersky Endpoint Security for Windows, os seguintes eventos serão exibidos na lista de eventos:

- **Inicialização do aplicativo proibida** (evento *Crítico*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para aplicar regras.
- **Proibida a inicialização do aplicativo em modo de teste** (evento *Informativo*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para testar regras.
- **Mensagem ao administrador sobre a proibição de inicialização do aplicativo** (evento de *Advertência*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para aplicar regras e um usuário tiver solicitado acesso ao aplicativo bloqueado para inicialização.

É recomendável criar seleções de eventos para visualizar eventos relacionados à operação do Controle de Aplicativos.

Você pode adicionar arquivos executáveis relacionados aos eventos do Controle de Aplicativos à uma categoria de aplicativos existente ou a uma nova categoria de aplicativos. Você pode adicionar arquivos executáveis apenas à categoria de aplicativos com conteúdo adicionado manualmente.

Para adicionar arquivos executáveis relativos aos eventos de Controle de Aplicativos para uma categoria de aplicativos:

1. No menu principal, acesse **Monitoramento e relatórios → Seleções de eventos**.

   A lista de seleção de eventos é exibida.

2. Selecione a seleção de eventos para visualizar os eventos relacionados ao Controle de Aplicativos e iniciar essa seleção de eventos.

   Se você não criou uma seleção de eventos relacionada ao Controle de Aplicativos, poderá selecionar e iniciar uma seleção predefinida, por exemplo, **Eventos recentes**.

   A lista de eventos é exibida.

3. Selecione os eventos cujos arquivos executáveis associados você deseja adicionar à categoria de aplicativos e clique no botão **Atribuir à categoria**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

4. Na página do assistente, especifique as configurações relevantes:

- Na seção **Ação em arquivo executável relacionado ao evento**, selecione uma das seguintes opções:
  - Adicionar a uma nova categoria de aplicativos

    Selecione esta opção se desejar criar uma nova categoria de aplicativo com base nos arquivos executáveis relacionados ao evento.

    Por padrão, esta opção está selecionada.

    Se você selecionou esta opção, especifique um novo nome de categoria.

  - Adicionar a uma categoria de aplicativos existente

    Selecione esta opção se você quiser adicionar arquivos executáveis relativos ao evento a uma categoria de aplicativo existente.

    Por padrão, esta opção não está selecionada.

    Se você selecionou essa opção, selecione a categoria de aplicativo com conteúdo adicionado manualmente ao qual você deseja adicionar arquivos executáveis.

- Na seção **Tipo de regra**, selecione uma das seguintes opções:
  - **Regras para adicionar às inclusões**
  - **Regras para adicionar às exclusões**
- Na seção **Parâmetro usado como condição**, selecione uma das seguintes opções:
  - Detalhes do certificado (ou hashes SHA-256 para arquivos sem certificado)

    Os arquivos podem ser assinados com um certificado. Múltiplos arquivos podem ser assinados com o mesmo certificado. Por exemplo, as versões diferentes do mesmo aplicativo podem ser assinadas com o mesmo certificado, ou diversos aplicativos diferentes do mesmo fornecedor podem ser assinados com o mesmo certificado. Quando você seleciona um certificado, diversas versões de um aplicativo ou diversos aplicativos do mesmo fornecedor podem terminar na categoria.

    Cada arquivo tem a sua própria função SHA-256 hash única. Quando você seleciona uma função SHA-256 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

    Selecione esta opção se você quiser adicionar às regras de categoria os detalhes do certificado de um arquivo executável (ou a função SHA-256 hash de arquivos sem um certificado).

    Por padrão, esta opção está selecionada.

  - Detalhes do certificado (arquivos sem um certificado serão ignorados)

    Os arquivos podem ser assinados com um certificado. Múltiplos arquivos podem ser assinados com o mesmo certificado. Por exemplo, as versões diferentes do mesmo aplicativo podem ser assinadas com o mesmo certificado, ou diversos aplicativos diferentes do mesmo fornecedor podem ser assinados com o mesmo certificado. Quando você seleciona um certificado, diversas versões de um aplicativo ou diversos aplicativos do mesmo fornecedor podem terminar na categoria.

    Selecione esta opção se você quiser adicionar os detalhes do certificado de um arquivo executável às regras de categoria. Se o arquivo executável não tiver um certificado, este arquivo será ignorado. Nenhuma informação sobre este arquivo será adicionada à categoria.

- **Somente SHA-256 (arquivos sem hash serão ignorados)**

  Cada arquivo tem a sua própria função SHA-256 hash única. Quando você seleciona uma função SHA-256 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

  Selecione esta opção se você quiser adicionar somente os detalhes da função SHA-256 hash do arquivo executável.

- **Somente MD5 (modo descontinuado, somente para a versão Kaspersky Endpoint Security 10 Service Pack 1)**

  Cada arquivo tem a sua própria função MD5 hash única. Quando você seleciona uma função MD5 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

  Selecione esta opção se você quiser adicionar somente os detalhes da função MD5 hash do arquivo executável. O cálculo função MD5 hash é suportado por versões do Service Pack 1 do Kaspersky Endpoint Security 10 for Windows e posteriores.

5. Clique em **OK**.

Quando o assistente for concluído, os arquivos executáveis relacionados aos eventos do Controle de Aplicativos serão adicionados à categoria de aplicativos existente ou a uma nova categoria de aplicativos. Você pode visualizar as configurações da categoria de aplicativos que modificou ou criou.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux

Criação de um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky

O Kaspersky Security Center Web Console permite executar a instalação remota de aplicativos de terceiros usando pacotes de instalação. Esses aplicativos de terceiros são incluídos em um banco de dados dedicado da Kaspersky.

A criação de pacotes de instalação de aplicativos de terceiros a partir do banco de dados da Kaspersky está disponível apenas sob a licença de gerenciamento de vulnerabilidades e patches.

Para criar um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky:

1. No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**.
2. Clique no botão **Adicionar**.
3. Na página do Assistente de novo pacote aberta, selecione a opção **Selecione um aplicativo no banco de dados da Kaspersky para criar um pacote de instalação** e clique em **Avançar**.

4. Na lista de aplicativos aberta, selecione o aplicativo relevante e clique em **Avançar**.

5. Selecione o idioma de localização relevante na lista suspensa e clique em **Avançar**.

   Esta etapa só será exibida se o aplicativo oferecer várias opções de idioma.

6. Se for solicitado que você aceite um Contrato de Licença para a instalação, na página **Contrato de Licença de Usuário Final** que é aberta, clique no link para ler o Contrato de Licença no site do fornecedor e selecione a caixa de seleção **Eu confirmo que li, compreendo e aceito integralmente os termos e condições deste Contrato de Licença de Usuário Final**.

7. Na página **Nome do novo pacote de instalação** aberta, no campo **Nome do pacote**, digite o nome do pacote de instalação e clique em **Avançar**.

Aguarde até que o pacote de instalação recém-criado seja carregado no Servidor de Administração. Quando o Assistente de novo pacote exibir a mensagem de que o processo de criação do pacote foi realizado com êxito, clique em **Concluir**.

O pacote de instalação recém-criado aparece na lista de pacotes de instalação. Você pode selecionar esse pacote ao criar ou reconfigurar a tarefa *Instalar aplicativo remotamente*.

Ver e modificar as configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky

Se você já criou algum pacote de instalação de aplicativos de terceiros listados no banco de dados da Kaspersky, poderá visualizar e modificar as configurações desse pacote posteriormente.

A modificação das configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky está disponível apenas para a licença de Gerenciamento de patches e vulnerabilidades.

Para visualizar e modificar as configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky:

1. No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**.

2. Na lista de pacotes de instalação aberta, clique no nome do pacote relevante.

3. Na página de propriedades aberta, modifique as configurações, conforme necessário.

4. Clique no botão **Salvar**.

As configurações que você modificou são salvas.

Configurações do pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky

As configurações do pacote de instalação de um aplicativo de terceiros são agrupadas nas seguintes guias:

Apenas uma parte das configurações listadas abaixo são exibidas por padrão, então você pode adicionar as colunas correspondentes clicando no botão **Filtro** e selecionando nomes de colunas relevantes da lista.

- Guia **Geral**:
  - Campo de entrada que contém o nome do pacote de instalação que pode ser editado manualmente
  - Aplicativo

    O nome do aplicativo de terceiros para o qual o pacote de instalação foi criado.
  - Versão

    O número da versão do aplicativo de terceiros para o qual o pacote de instalação foi criado.
  - Tamanho

    O tamanho do pacote de instalação de terceiros (em kilobytes).
  - Criação

    A data e hora em que o pacote de instalação de terceiros foi criado.
  - Caminho

    O caminho para a pasta de rede em que o pacote de instalação de terceiros está localizado.
- Guia **Procedimento de instalação**:
  - Instalar os componentes gerais do sistema necessários

    Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional.

    Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

    Por padrão, esta opção está desativada.
  - Tabela que exibe as propriedades de atualização e contendo as seguintes colunas:
    - Nome

      O nome da atualização.
    - Descrição

      A descrição da atualização.

- **Origem**

  A fonte da atualização, isto é, se foi lançada pela Microsoft ou por outro desenvolvedor terceiro.

- **Tipo**

  O tipo da atualização, ou seja, se é destinada a um driver ou aplicativo.

- **Categoria**

  A categoria WSUS (Windows Server Update Services) exibida para atualizações da Microsoft (atualizações críticas, atualizações de definições, drivers, pacotes de recursos, atualizações de segurança, service packs, ferramentas, pacotes cumulativos de atualizações, atualizações ou upgrades).

- **Nível de importância de acordo com o MSRC**

  O nível de importância da atualização definido pelo Microsoft Security Response Center (MSRC).

- **Nível de importância**

  O nível de importância da atualização definido pela Kaspersky.

- **Nível de importância do patch**

  O nível de importância do patch caso se destine a um aplicativo Kaspersky.

- **Artigo**

  O identificador (ID) do artigo na Base de Conhecimento que descreve a atualização.

- **Boletim**

  O ID do boletim de segurança que descreve a atualização.

- **Não atribuído para a instalação (nova versão)**

  Exibe se a atualização tem o status Não atribuída para instalação.

- **A ser instalado**

  Exibe se a atualização tem o status A ser instalada.

- **Instalando**

  Exibe se a atualização tem o status Instalando.

- **Instalado**

Exibe se a atualização tem o status Instalada.

- **Falhou**

  Exibe se a atualização tem o status Falha.

- **A reinicialização é necessária**

  Exibe se a atualização tem o status Reinicialização necessária.

- **Registrado**

  Exibe a data e a hora em que a atualização foi registrada.

- **Instalado no modo interativo**

  Exibe se a atualização requer interação com o usuário durante a instalação.

- **Revogado**

  Exibe a data e a hora em que a atualização foi revogada.

- **Status de aprovação da atualização**

  Exibe se a atualização está aprovada para instalação.

- **Revisão**

  Exibe o número da revisão atual da atualização.

- **ID de atualização**

  Exibe o ID da atualização.

- **Versão do aplicativo**

  Exibe o número da versão para a qual o aplicativo deve ser atualizado.

- **Substituído**

  Exibe outras atualizações que podem substituir a atualização.

- **Substituição**

  Exibe outras atualizações que podem ser substituídas pela atualização.

- **Você deve aceitar os termos do Contrato de Licença**

Exibe se a atualização requer aceitação dos termos de um Contrato de Licença do Usuário Final (EULA).

- URL de descrição

  Exibe o nome do fornecedor da atualização.

- Família do aplicativo

  Exibe o nome da família de aplicativos à qual a atualização pertence.

- Aplicativo

  Exibe o nome do aplicativo ao qual a atualização pertence.

- Idioma da localização

  Exibe o idioma da localização da atualização.

- Não atribuído para a instalação (nova versão)

  Exibe se a atualização tem o status Não atribuída para instalação (nova versão).

- Requer a instalação de pré-requisitos

  Exibe se a atualização tem o status de instalação Requer pré-requisitos.

- Modo de download

  Exibe o modo de download da atualização.

- É um patch

  Exibe se a atualização é um patch.

- Não instalado

  Exibe se a atualização tem o status Não instalada.

- Guia **Configurações** que exibe as configurações do pacote de instalação, com seus nomes, descrições e valores usados como parâmetros de linha de comando durante a instalação. Se o pacote não fornecer estas configurações, a mensagem correspondente será exibida. Você pode modificar os valores destas configurações.

- Guia **Histórico de revisões** que exibe as revisões do pacote de instalação e contém as seguintes colunas:

  - Revisão

    Exibe o número da revisão dos pacotes de instalação.

- **Hora**

  Exibe a hora em que a revisão foi criada.

- **Usuário**

  Exibe o nome da conta do usuário sob a qual a revisão foi criada.

- **Ação**

  Lista as ações executadas no pacote de instalação dentro da revisão.

- **Descrição**

  Exibe a descrição de texto adicionada para a revisão.

Tags de aplicativo

Esta seção descreve as tags do aplicativo e fornece instruções para criá-los e modificá-los, bem como para aplicar tag em aplicativos de terceiros.

Sobre as tags de aplicativos

O Kaspersky Security Center Cloud Console permite aplicar tag a aplicativos de terceiros (aplicativos criados por fornecedores de software além da Kaspersky). Uma tag é o rótulo de um aplicativo que pode ser usada para agrupar ou encontrar dispositivos. Uma tag destinada a aplicativos pode servir como uma condição em seleções de dispositivos.

Por exemplo, você pode criar a tag `[Browsers]` e atribuí-la a todos os navegadores, como Microsoft Internet Explorer, Google Chrome, Mozilla Firefox etc.

Criando uma tag de aplicativo

Para criar um tag de aplicativo:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Tags de aplicativos**.
2. Clique em **Adicionar**.

   Uma nova janela de tag é exibida.
3. Insira o nome da tag.
4. Clique em **OK** para salvar as alterações.

A nova tag aparece na lista de tags de aplicativos.

Renomeando uma tag de aplicativo

Para renomear um identificador de aplicativos:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Tags de aplicativos**.
2. Marque a caixa de seleção ao lado do identificador que deseja renomear e clique em **Editar**.

   A janela de propriedades do identificador é exibida.
3. Altere o nome do identificador.
4. Clique em **OK** para salvar as alterações.

A tag atualizado aparece na lista de tags de aplicativos.

Atribuindo uma tag de aplicativos

Para atribuir uma ou várias tags a um aplicativo:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Registro de aplicativos**.
2. Clique no nome do aplicativo ao qual deseja atribuir tags.
3. Selecione a guia **Tags**.

   A guia exibe todos as tags de aplicativos existentes no Servidor de Administração. Para tags atribuídas ao aplicativo selecionado, a caixa de seleção na coluna **Tag atribuída** é selecionada.
4. Para as tags que deseja atribuir, marque as caixas de seleção na coluna **Tag atribuída**.
5. Clique em **Salvar** para salvar as alterações.

As tags são atribuídas ao aplicativo.

Removendo tags atribuídas de um aplicativo

Para remover uma ou várias tags de um aplicativo:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Registro de aplicativos**.
2. Clique no nome do aplicativo do qual deseja remover tags.
3. Selecione a guia **Tags**.

   A guia exibe todos as tags de aplicativos existentes no Servidor de Administração. Para tags atribuídas ao aplicativo selecionado, a caixa de seleção na coluna **Tag atribuída** é selecionada.
4. Para tags que deseja remover, desmarque as caixas de seleção na coluna **Tag atribuída**.

5. Clique em **Salvar** para salvar as alterações.

As tags são removidas do dispositivo.

As tags de aplicativos removidas não são excluídas. Se quiser, você pode excluí-los manualmente.

Excluir uma tag de aplicativos

Para excluir um identificador de aplicativos:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Tags de aplicativos**.
2. Na lista, selecione o identificador de aplicativos que deseja excluir.
3. Clique no botão **Excluir**.
4. Na janela que se abre, clique em **OK**.

O identificador de aplicativos é excluído. O identificador excluído é automaticamente removido de todos dos aplicativos aos quais foi atribuído.

Configurando o Servidor de Administração

Esta seção descreve o processo de configuração e as propriedades do Servidor de Administração do Kaspersky Security Center.

Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de Administração secundário

É possível fazer um Servidor de Administração em execução no local funcionar como um Servidor de Administração secundário, estabelecendo, assim, uma hierarquia "principal/secundário" na rede. Para o Servidor de Administração na infraestrutura da Kaspersky, os Servidores de Administração principal e secundário em sua rede são Servidores secundários. Você pode adicionar um Servidor de Administração baseado em Windows, bem como um Servidor de Administração baseado em Linux.

Para adicionar um Servidor de Administração secundário que esteja disponível para a conexão:

1. Certifique-se de que o futuro Servidor de Administração secundário tenha o Kaspersky Security Center Web Console instalado.

2. No futuro Servidor de Administração secundário, baixe e salve o certificado do Servidor de Administração para que seja possível adicioná-lo ao Servidor de Administração principal em uma das etapas do Assistente para Adicionar Servidor de Administração secundário.

3. Execute as seguintes ações por meio do Kaspersky Security Center Web Console no futuro Servidor de Administração secundário (ou solicite que o administrador do futuro Servidor de Administração secundário execute estas ações):

    a. No menu principal, clique no ícone de Configurações ( ) ao lado do nome do futuro Servidor de Administração secundário.

    b. Na página de propriedades que se abre, prossiga para a seção **Hierarquia de Servidores de Administração** da guia **Geral**.

    c. Selecione a opção **Esse Servidor de Administração é secundário na hierarquia**.

    d. Selecione **Cloud Console** como o tipo do Servidor de Administração principal.

    Os campos de configuração para estabelecer a conexão entre os Servidores de Administração secundários e principais tornam-se disponíveis.

    e. Nos campos **Endereço do servidor HDS (do Servidor de Administração Principal no Cloud Console)** e **Portas do servidor HDS**, insira o endereço e a porta do servidor de administração principal do Kaspersky Security Center Cloud Console.

    É possível encontrar o endereço do servidor HDS e a porta do servidor HDS no Servidor de Administração do Kaspersky Security Center Cloud Console, na seção **Hierarquia de Servidores de Administração** da guia **Geral** da janela de propriedades. Você pode copiar e colar esses dados nos campos da janela do Servidor de Administração secundário.

    f. Clique no botão **Especifique o certificado do Servidor de Administração Principal** e, em seguida, selecione o certificado.

    É possível baixar o certificado do Servidor de Administração do Kaspersky Security Center Cloud Console na seção **Hierarquia de Servidores de Administração** da guia **Geral** da janela de propriedades clicando no botão **Visualizar o certificado do Servidor de Administração**.

g. Clique no botão **Especifique os certificados do Serviço de Descoberta Hospedada** e selecione o certificado.

É possível baixar esse certificado do Servidor de Administração do Kaspersky Security Center Cloud Console na seção **Hierarquia de Servidores de Administração** na guia **Geral** da janela de propriedades, clicando no botão **HDS root CA certificate**.

h. Se você usar um servidor proxy para conectar o Servidor de Administração do Kaspersky Security Center Cloud Console (ou seja, o servidor principal na hierarquia), especifique-o e insira as credenciais do servidor proxy.

i. Selecione a opção **Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ** caso o Servidor de Administração secundário esteja em uma zona desmilitarizada.

j. Clique **Save** para salvar as alterações e sair da janela.

4. No menu principal, clique no ícone de Configurações ( ) ao lado do nome do futuro Servidor de Administração principal.

5. Na página de propriedades que se abre, clique na guia **Servidores de Administração**.

6. Marque a caixa de seleção ao lado do nome do grupo de administração ao qual deseja adicionar o Servidor de Administração secundário.

7. Na linha de menu, clique em **Conectar Servidor de Administração secundário**.

O assistente para Adicionar Servidor de Administração secundário é iniciado.

8. Na primeira página do assistente, preencha os seguintes campos:

- Nome de exibição do Servidor de Administração secundário

  O nome designado para o Servidor de Administração secundário será exibido na hierarquia. Se desejar, você pode inserir o endereço IP como um nome ou pode usar um nome como "Servidor secundário para o grupo 1".

- Endereço do Servidor de Administração secundário (opcional)

  Especifique o endereço IP ou o nome de domínio do Servidor de Administração secundário.

  Esse parâmetro será obrigatório se a opção **Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ** estiver ativada.

9. Se você usar um servidor proxy para conectar o Servidor de Administração do Kaspersky Security Center Cloud Console (ou seja, o futuro servidor principal), especifique isso e insira as credenciais do servidor proxy.

10. Siga as instruções do assistente.

Após a conclusão do assistente, a hierarquia "principal/secundário" é criada. O Servidor de Administração principal começa a receber a conexão do Servidor de Administração secundário pela porta 13000. As tarefas e as políticas do Servidor de Administração principal são recebidas e aplicadas. O Servidor de Administração secundário é exibido no Servidor de Administração principal, no grupo de administração ao qual foi adicionado.

Criação de grupos de administração

Inicialmente, a hierarquia de grupos de administração contém apenas um grupo de administração chamado grupo de **Dispositivos gerenciados**. É possível adicionar dispositivos e subgrupos em um grupo de **Dispositivos gerenciados**.

Para criar um grupo de administração:

1. No menu principal, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Na hierarquia, selecione o grupo de administração que deve incluir o novo grupo de administração.
3. Clique no botão **Adicionar**.
4. Na janela que será aberta, insira um nome para o grupo e clique em **Adicionar**.

Um novo grupo de administração com o nome especificado aparece na hierarquia do grupo de administração.

O aplicativo permite criar a hierarquia dos grupos de administração com base na estrutura do Active Directory ou na estrutura de domínio da rede. Você também pode criar uma estrutura de grupos a partir de um arquivo de texto.

Para criar a estrutura de grupos de administração:

1. No menu principal, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Clique no botão **Importar**.

O Assistente de Nova Estrutura de Grupos de Administração é iniciado. Siga as instruções do Assistente.

Configurando o prazo de armazenamento de eventos relativos aos dispositivos excluídos

No Kaspersky Security Center Cloud Console, os eventos são armazenados em um repositório de eventos. Você não pode configurar quantos eventos armazenar no repositório de eventos.

Na seção **Repositório de eventos** da janela de propriedades do Servidor de Administração, você pode configurar o prazo máximo de armazenamento de eventos relacionados aos dispositivos excluídos. O prazo máximo de armazenamento é de 1.000 dias.

Para configurar o número de dias para armazenar eventos relacionados aos dispositivos excluídos:

1. No menu principal, clique no ícone de Configurações ( ) ao lado do Servidor de Administração do Kaspersky Security Center Cloud Console.

   A janela Propriedades do Servidor de Administração é aberta.
2. Na guia **Geral**, selecione a seção **Repositório de eventos**.
3. Ative a opção **Armazenar eventos após a exclusão dos dispositivos**.

4. Na caixa de edição **Período máximo de armazenamento (dias)**, especifique o número de dias para armazenar eventos relacionados aos dispositivos excluídos.

   O número de dias para armazenar eventos relacionados aos dispositivos excluídos é limitado pelo valor especificado.

Além disso, é possível alterar as configurações de qualquer tarefa para salvar eventos relacionados ao andamento da tarefa ou salvar apenas os resultados de execução da tarefa. Ao fazer isso, você reduzirá o número de eventos no banco de dados, aumentará a velocidade da execução dos cenários associados com a análise da tabela de eventos no banco de dados e abaixará o risco de que os eventos críticos sejam substituídos por um grande número de eventos.

Agregar e-mails sobre eventos

Durante a operação, o Kaspersky Security Center Cloud Console e os aplicativos gerenciados da Kaspersky geram eventos. Cada evento é atribuído a um determinado tipo e nível de gravidade (*Crítico*, *Falha funcional*, *Aviso* ou *Informativo*). Dependendo das condições sob as quais um evento ocorreu, o Kaspersky Security Center Cloud Console pode atribuir diferentes níveis de gravidade aos eventos do mesmo tipo.

O Kaspersky Security Center Cloud Console envia automaticamente por e-mail notificações sobre eventos. O Kaspersky Security Center Cloud Console envia notificações sobre os eventos listados na janela de **Propriedades do Servidor de Administração**, na guia **Configuração de eventos**. Configurações de notificação comuns são usadas para todos os tipos de eventos.

Para limitar o número de e-mails que precisam ser enviados, o Kaspersky Security Center Cloud Console, durante períodos específicos, agrega eventos com o mesmo nível de gravidade. Os valores dos períodos são gerenciados por especialistas da Kaspersky. Como resultado, os destinatários recebem mensagens de e-mails agregados de acordo com o seguinte modelo: "<Number><Severity_level> (e de nível inferior) ocorreram".

Limitações no gerenciamento de Servidores de Administração secundários em execução no local através do Kaspersky Security Center Cloud Console

Depois de alternar para um Servidor de Administração secundário em execução no local usando a opção correspondente no Kaspersky Security Center Cloud Console, o aplicativo impõe limitações específicas ao gerenciamento desse Servidor de Administração secundário. As seguintes configurações relacionadas à operação do Kaspersky Security Center Cloud Console ficam indisponíveis para o usuário:

- Nas configurações das políticas do Agente de Rede e do Servidor de Administração, as guias **Configuração de eventos** e **Configurações do aplicativo** não estão disponíveis. Nenhuma nova política pode ser criada.
- Nas configurações das tarefas do Agente de Rede e do Servidor de Administração, as guias **Configuração de eventos** e **Configurações do aplicativo** não estão disponíveis. Nenhuma nova tarefa pode ser criada.
- O gerenciamento do Agente de Rede e do Servidor de Administração está indisponível, assim como a janela de propriedades do Servidor de Administração secundário.
- O Assistente de Início Rápido está indisponível.
- As configurações de armazenamento e notificação para eventos do Agente de Rede e do Servidor de Administração não podem ser modificadas.

- A seção **Versões atuais do aplicativo** está indisponível.
- A seção **Pacotes de instalação** está indisponível.

Visualizar a lista de Servidores de administração secundários

Para visualizar a lista de Servidores de administração secundários (incluindo virtuais):

No menu principal, clique no nome do Servidor de Administração ao lado do ícone de configurações ( ).

A lista suspensa dos Servidores de administração secundários (incluindo virtuais) é exibida.

Você pode prosseguir para qualquer um desses Servidores de Administração clicando no nome.

Excluir uma hierarquia de Servidores de Administração

Se você não quiser mais ter uma hierarquia de Servidores de Administração, você poderá desconectá-los dessa hierarquia.

Para excluir uma hierarquia de Servidores de Administração:

1. No menu principal, clique no ícone de Configurações ( ) ao lado do nome do Servidor de Administração principal.
2. Na página que se abre, prossiga para a guia **Servidores de Administração**.
3. No grupo de administração do qual deseja excluir o Servidor de administração secundário, selecione o Servidor de administração secundário.
4. Na linha de menu, clique em **Excluir**.
5. Na janela que se abre, clique em **OK** para confirmar que deseja excluir o Servidor de administração secundário.

Os antigos Servidores de administração principal e secundário agora são independentes um do outro. A hierarquia não existe mais.

Configurar interface

Você pode configurar a interface do Kaspersky Security Center Cloud Console para exibir e ocultar seções e elementos da interface, dependendo dos recursos usados.

Para configurar a interface do Kaspersky Security Center Cloud Console de acordo com o conjunto de recursos usados no momento:

1. No menu principal, acesse as configurações da conta e selecione **Opções da interface.**

2. Na janela **Opções da interface** exibida, ative ou desative as opções:

   - **Mostrar a criptografia e proteção de dados**

     Você pode usar esta opção para ocultar ou exibir a seção **Operações → Criptografia e proteção de dados** na interface. O Kaspersky Security Center Cloud Console salva o valor desta opção apenas para sua própria conta de usuário, enquanto o outro usuário pode definir um valor diferente.

   - **Exibir recursos MDR**

     Você pode usar esta opção para ocultar ou exibir a seção **Monitoramento e relatórios → Incidentes** na interface. O Kaspersky Security Center Cloud Console salva o valor desta opção apenas para sua própria conta de usuário, enquanto o outro usuário pode definir um valor diferente.

3. Defina a quantidade de dispositivos que o Kaspersky Security Center Cloud Console exibe em resultados de distribuição de políticas.

4. Clique em **Salvar**.

As configurações da interface do console são definidas de acordo com suas preferências.

Gerenciar Servidores de Administração virtuais

Esta seção descreve as seguintes ações para gerenciar Servidores de Administração virtuais:

- Criar Servidores de Administração virtuais
- Ativar ou desativar de Servidores de Administração virtuais
- Atribuir um administrador para um Servidor de Administração virtual
- Alterar o Servidor de Administração para dispositivos cliente
- Excluir Servidores de Administração virtuais

Criar um Servidor de Administração virtual

Você pode criar Servidores de Administração virtuais e adicioná-los a grupos de administração.

Para criar e adicionar um Servidor de Administração virtual:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

2. Na página que se abre, prossiga para a guia **Servidores de Administração**.

3. Selecione o grupo de administração ao qual você deseja adicionar um Servidor de Administração virtual.

4. Na linha de menu, clique em **Novo Servidor de Administração virtual**.

5. Na página aberta, defina o **Nome do Servidor de Administração virtual**.

6. Clique em **Salvar**.

O novo Servidor de Administração virtual é criado, adicionado ao grupo de administração e exibido na guia **Servidores de Administração**.

Ativando ou desativando um Servidor de Administração virtual

Ao criar um novo Servidor de Administração virtual, ele é ativado por padrão. Você pode desativá-lo ou ativá-lo novamente a qualquer momento. Desativar ou ativar um Servidor de Administração virtual é igual a desligar ou ligar um Servidor de Administração físico.

Para ativar ou desativar um Servidor de Administração virtual:

1. No menu principal, clique no ícone de configurações () ao lado do nome do Servidor de Administração necessário.

2. Na página que se abre, prossiga para a guia **Servidores de Administração**.

3. Selecione o Servidor de Administração virtual que deseja ativar ou desativar.

4. Na linha do menu, clique no botão **Ativar/desativar Servidor de Administração virtual**.

O estado do Servidor de Administração virtual é alterado para ativado ou desativado, dependendo da condição anterior. O estado atualizado é exibido próximo ao nome do Servidor de Administração.

Atribuição de um administrador para um Servidor de Administração virtual

Ao usar Servidores de Administração virtuais em sua organização, convém atribuir um administrador dedicado para cada Servidor de Administração virtual. Por exemplo, isso pode ser útil quando os Servidores de Administração virtuais são criados para gerenciar escritórios ou departamentos separados de sua organização, ou se você for um provedor de MSP e gerenciar locatários por meio de Servidores de Administração virtuais.

Quando um Servidor de Administração virtual é criado, ele herda a lista de usuários e todos os direitos de usuário do Servidor de Administração principal. Caso um usuário tenha direitos de acesso ao servidor principal, esse usuário também terá direitos de acesso ao servidor virtual. Após a criação, é preciso configurar os direitos de acesso aos Servidores de forma independente. Caso queira apenas atribuir um administrador para um Servidor de Administração virtual, verifique e confirme se o administrador não está incluído na lista de **Direitos de acesso** nas propriedades do Servidor de Administração principal.

É possível atribuir um administrador para um Servidor de Administração virtual concedendo os direitos de acesso de administrador ao Servidor de Administração virtual. É possível conceder os direitos de acesso necessários das seguintes formas:

- Configure os direitos de acesso para o administrador manualmente
- Atribua uma ou mais funções de usuário ao administrador

Ao atribuir um administrador, certifique-se de ter concedido acesso a um único Servidor de Administração virtual. Um administrador com acesso a vários Servidores de Administração virtuais não pode fazer login no Kaspersky Security Center Cloud Console.

Um administrador de um Servidor de Administração virtual faz login no Kaspersky Security Center Cloud Console da mesma forma que faz login no Servidor de Administração principal. O Kaspersky Security Center Cloud Console autentica o administrador e abre o Servidor de Administração virtual ao qual o administrador tem direitos de acesso. O administrador não pode alternar entre os Servidores de Administração.

Pré-requisitos

Antes de iniciar, certifique-se de que as seguintes condições sejam atendidas:

- O Servidor de Administração virtual foi criado.
- No Servidor de Administração principal, foi criada uma conta para o administrador que se deseja atribuir ao Servidor de Administração virtual.
- A conta criada do administrador do servidor virtual não está incluída nas listas de **Direitos de acesso** nas propriedades de nenhum servidor, principal ou secundário.
- O usuário tem o direto de **Modificar os objetos ACLs** na área funcional **Funcionalidades gerais → Permissões do usuário**.

Configuração dos direitos de acesso manualmente

Para atribuir um administrador para um Servidor de Administração virtual:

1. No menu principal, alterne para o Servidor de Administração virtual necessário:
   a. Clique no ícone de sinalização ( ) à direita do nome atual do Servidor de Administração.
   b. Selecione o Servidor de Administração necessário.
2. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.
   A janela Propriedades do Servidor de Administração é aberta.
3. Na guia **Direitos de acesso**, clique no botão **Adicionar**.
   Uma lista unificada de usuários do Servidor de Administração principal e do Servidor de Administração virtual atual é aberta.
4. Na lista de usuários, selecione a conta do administrador que deseja atribuir ao Servidor de Administração virtual e clique no botão **OK**.
   O aplicativo adiciona o usuário selecionado à lista de usuários na aba **Direitos de acesso**.
5. Marque a caixa de seleção ao lado de conta adicionada e clique no botão **Direitos de acesso**.
6. Configure os direitos que o administrador terá no Servidor de Administração virtual.
   Para uma autenticação bem-sucedida, no mínimo, o administrador deve ter os seguintes direitos:
   - Direito de **Ler** na área funcional **Funcionalidades gerais → Funcionalidade básica**
   - Direito de **Ler** na área funcional **Funcionalidades gerais → Servidores de Administração virtuais**

O aplicativo salva os direitos de usuário modificados na conta do administrador.

Configuração de direitos de acesso com a atribuição de uma função de usuário

Como alternativa, é possível conceder direitos de acesso a um administrador do Servidor de Administração virtual por meio de funções de usuário. Por exemplo, isso pode ser útil caso se queira atribuir vários administradores no mesmo Servidor de Administração virtual. Se esse for o caso, é possível atribuir às contas dos administradores a mesma função de usuário, em vez de configurar os mesmos direitos de usuário para vários administradores.

Para atribuir um administrador para um Servidor de Administração virtual por meio da atribuição da função de usuário:

1. No Servidor de Administração principal, crie uma nova função de usuário e especifique todos os direitos de acesso necessários que um administrador deve ter no Servidor de Administração virtual. É possível criar várias funções, por exemplo, caso queira separar o acesso a diferentes áreas funcionais.
2. No menu principal, alterne para o Servidor de Administração virtual necessário:
   a. Clique no ícone de sinalização ( ) à direita do nome atual do Servidor de Administração.
   b. Selecione o Servidor de Administração necessário.
3. Atribuir a nova função ou diversas funções à conta de administrador.

O aplicativo atribui a nova função à conta de administrador.

Configuração de direitos de acesso no nível do objeto

Além de atribuir os direitos de acesso no nível de uma área funcional, é possível configurar o acesso a objetos específicos no Servidor de Administração virtual, por exemplo, para um grupo de administração específico ou uma tarefa. Para isso, alterne para o Servidor de Administração virtual e configure os direitos de acesso nas propriedades do objeto.

Excluindo um Servidor de Administração virtual

Ao excluir um Servidor de Administração virtual, todos os objetos criados no Servidor de Administração, incluindo políticas e tarefas, também são excluídos. Os dispositivos gerenciados dos grupos de administração gerenciados pelo Servidor de Administração virtual serão removidos dos grupos de administração. Para retornar os dispositivos sob gerenciamento do Kaspersky Security Center Cloud Console, execute a pesquisa de rede e migre os dispositivos encontrados do grupo Dispositivos não atribuídos para os grupos de administração.

Para excluir um Servidor de Administração virtual:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.
2. Na página que se abre, prossiga para a guia **Servidores de Administração**.
3. Selecione o Servidor de Administração virtual que deseja excluir.
4. Na linha do menu, clique no botão **Excluir**.

O Servidor de Administração virtual é excluído.

Monitoramento e relatórios

Esta seção descreve os recursos de monitoramento e emissão de relatórios do Kaspersky Security Center Cloud Console. Esses recursos fornecem a você uma visão geral da infraestrutura, dos status de proteção e das estatísticas.

Após a implementação do Kaspersky Security Center Cloud Console ou durante a operação, você pode configurar os recursos de monitoramento e emissão de relatórios de forma a atender melhor às suas necessidades.

Cenário: Monitoramento e relatórios

Esta seção fornece um cenário para a configuração do recurso de monitoramento e de relatórios no Kaspersky Security Center Cloud Console.

Pré-requisitos

Após ter implementado o Kaspersky Security Center Cloud Console na rede de uma organização, você poderá iniciar o seu monitoramento e gerar relatórios sobre o seu funcionamento.

Fases

A configuração do monitoramento e da geração de relatórios na rede de uma organização ocorre em fases:

1. **Configurar a alternância dos status do dispositivo**

   Conheça as configurações para os status do dispositivo dependendo de condições específicas. Modificando essas configurações, é possível alterar o número de eventos com os níveis de importância Crítico ou Aviso. Ao configurar a alternância dos status do dispositivo, esteja seguro do seguinte:

   - As novas configurações não entram em conflito com as políticas de segurança de informações da sua organização.
   - Você pode reagir a eventos de segurança importantes na rede da sua organização de maneira oportuna.

2. **Configurar as notificações de eventos em dispositivos cliente**

   Instruções de uso: Configurar a notificação (por e-mail) de eventos em dispositivos cliente

3. **Alteração da resposta da sua rede de segurança para o evento de Surto de vírus**

   Você pode alterar os limites específicos nas propriedades do Servidor de Administração. Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência do evento.

4. **Análise do status de segurança da rede da sua organização**

   Instruções de como proceder:

   - Revise o widget **Status da proteção**
   - Gere e analise o **Relatório do status da proteção**
   - Gere e analise o **Relatório de erros**

5. **Localize dispositivos cliente que não estão protegidos**

   Instruções de como proceder:

   - Analisar o widget **Novos dispositivos**
   - Gere e analise o **Relatório de implementação de proteção**

6. **Verificação da proteção de dispositivos cliente**

   Instruções de como proceder:

   - Gere e revise os relatórios das categorias **Status da proteção** e **Estatísticas de ameaças**
   - Inicie e analise a seleção de eventos do tipo **Crítico**

7. **Análise de informações de licença**

   Instruções de como proceder:

   - Adicione o widget de **Uso de chaves de licença** ao painel e analise-o
   - Gere e analise o **Relatório de uso das chaves de licença**

Resultados

Após a conclusão do cenário, você é informado sobre a proteção da rede da sua organização e, portanto, poderá planejar ações para proteção adicional.

Sobre os tipos do monitoramento e relatórios

As informações sobre eventos de segurança na rede de uma organização são armazenadas no banco de dados do Servidor de Administração. Com base nos eventos, o Kaspersky Security Center Cloud Console fornece os seguintes tipos de monitoramento e relatórios na rede da sua organização:

- Painel
- Relatórios
- Seleções de eventos

Painel

O painel permite monitorar tendências de segurança na rede da sua organização fornecendo uma exibição gráfica das informações.

Relatórios

O recurso Relatórios permite obter informações numéricas detalhadas sobre a segurança da rede da sua organização, salvar essas informações em um arquivo, enviá-las por e-mail e imprimi-las.

Seleções de eventos

As seleções de evento fornecem uma visualização na tela de conjuntos nomeados de eventos selecionados do banco de dados do Servidor de Administração. Esses conjuntos de eventos são agrupados de acordo com as seguintes categorias:

- Por nível de importância – **Eventos críticos**, **Falhas funcionais**, **Advertências** e **Eventos de informações**
- Por tempo – **Eventos recentes**
- Por tipo – **Pedidos de usuário** e **Eventos de auditoria**

Você pode criar e visualizar seleções de eventos definidos por usuários, com base nas configurações disponíveis, na interface do Kaspersky Security Center Cloud Console.

Painel e widgets

Esta seção contém informações sobre o painel e os widgets que o painel fornece. A seção inclui instruções sobre como gerenciar e definir as configurações dos widgets.

Usar o painel

O painel permite monitorar tendências de segurança na rede da sua organização fornecendo uma exibição gráfica das informações.

O painel está disponível no Kaspersky Security Center Cloud Console, na seção **Monitoramento e relatórios** clicando em **Painel**.

O painel fornece widgets que podem ser personalizados. Você pode selecionar um grande número de widgets diferentes, apresentadas como gráficos de pizza ou gráficos de rosca, tabelas, gráficos, gráficos de barras e listas. As informações exibidas nos widgets são atualizadas automaticamente em um intervalo de dois minutos. O intervalo entre atualizações varia para widgets diferentes. Você pode atualizar dados sobre um widget manualmente a qualquer momento por meio do menu de configurações.

Por padrão, os widgets contém informações sobre todos os eventos armazenados no banco de dados do Servidor de Administração.

O Kaspersky Security Center Cloud Console tem um conjunto padrão de widgets para as seguintes categorias:

- **Status da proteção**
- **Implementação**
- **Atualizando**
- **Estatísticas de ameaças**
- **Outro**

Alguns widgets têm informações de texto com links. Você pode exibir informações detalhadas clicando em um link.

Ao configurar o painel, você pode adicionar os widgets de que precisa, ocultar widgets de que não precisa, modificar o tamanho ou a aparência de widgets, mover widgets e modificar suas configurações.

Adição de widgets ao painel

Para adicionar widgets ao painel:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no botão **Adicionar ou restaurar widget da Web**.
3. Na lista de widgets disponíveis, selecione os widgets que deseja adicionar ao painel.

   Os widgets são agrupados por categoria. Para visualizar a lista de widgets incluídos em uma categoria, clique no ícone de insígnia (>) ao lado do nome da categoria.
4. Clique no botão **Adicionar**.

Os widgets selecionados são adicionados no final do painel.

Você pode editar agora a representação e os parâmetros dos widgets adicionados.

Ocultação de um widget do painel

Para ocultar um widget exibido do painel:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja ocultar.
3. Selecione **Ocultar widget da Web**.
4. Na janela **Advertência** que se abre, clique em **OK**.

O widget selecionado fica oculto. Depois, você pode adicionar esse widget ao painel novamente.

Movimentação de um widget no painel

Para mover um widget no painel:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja mover.
3. Selecione **Migrar**.
4. Clique no lugar para o qual deseja mover o widget. Você pode selecionar apenas outro widget.

Os lugares dos widgets selecionados são trocados.

Alteração do tamanho ou da aparência do widget

Para widgets que exibem um gráfico, você pode alterar sua representação: um gráfico de barras ou um gráfico de linhas. Para alguns widgets, você pode alterar seu tamanho: compacto, médio ou máximo.

Para alterar a representação do widget:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja editar.
3. Execute uma das seguintes ações:
   - Para exibir o widget como um gráfico de barras, selecione **Tipo de gráfico: barras**.
   - Para exibir o widget como um gráfico de linhas, selecione **Tipo de gráfico: linhas**.
   - Para alterar a área ocupada pelo widget, selecione um dos valores:
     - **Compacto**
     - **Compacto (somente barra)**
     - **Médio (gráfico de rosca)**
     - **Médio (gráfico de barras)**
     - **Máximo**

A representação do widget selecionado é alterada.

Alteração das configurações do widget

Para alterar as configurações de um widget:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja alterar.
3. Selecione **Mostrar configurações**.
4. Na janela de configurações de widget exibida, modifique as configurações de widget conforme necessário.
5. Clique em **Salvar** para salvar as alterações.

As configurações do widget selecionado são alteradas.

O conjunto de configurações depende do widget específico. Abaixo estão algumas configurações comuns:

- **Escopo do widget da Web** (o conjunto de objetos para os quais o widget exibe informações): por exemplo, um grupo de administração ou uma seleção de dispositivos.
- **Selecionar tarefa** (a tarefa para a qual o widget exibe informações).
- **Intervalo de tempo** (o intervalo de tempo durante o qual as informações são exibidas no widget): entre as duas datas especificadas; desde a data especificada até o dia atual; ou do dia atual menos o número especificado de dias até o dia atual.
- **Se especificados, definir como Crítico** e **Se especificados, definir como Advertência** (as regras que determinam a cor de um semáforo).

Depois de alterar as configurações do widget, você pode atualizar os dados manualmente.

Para atualizar dados e um widget:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja mover.
3. Selecione **Atualizar**.

Os dados no widget são atualizados.

Sobre o modo somente painel

É possível configurar o modo somente painel para funcionários que não gerenciam a rede, mas que desejam visualizar as estatísticas de proteção da rede no Kaspersky Security Center Cloud Console (por exemplo, um gerente superior). Quando um usuário tem esse modo ativado, apenas um painel com um conjunto predefinido de widgets é exibido para o usuário. Assim, ele pode monitorar as estatísticas especificadas nos widgets, por exemplo, o status de proteção de todos os dispositivos gerenciados, o número de ameaças detectadas recentemente ou a lista das ameaças mais frequentes na rede.

Quando um usuário trabalha no modo somente painel, as seguintes restrições são aplicadas:

- O menu principal não é exibido para o usuário, portanto, ele não pode alterar as configurações de proteção de rede.
- O usuário não pode realizar nenhuma ação com widgets, por exemplo, adicioná-los ou ocultá-los. Portanto, não é necessário colocar todos os widgets requeridos para o usuário no painel e configurá-los, por exemplo, para definir a regra de contagem de objetos ou especificar o intervalo de tempo.

Não é possível atribuir o modo somente painel a si mesmo. Caso queira trabalhar nesse modo, entre em contato com um administrador do sistema, o Provedor de Serviços Gerenciados (MSP) ou um usuário com o direito **Modificar ACLs de objetos** na área funcional **Recursos gerais: Permissões do usuário**.

Configurando o modo somente painel

Antes de iniciar a configuração do Modo somente painel, verifique se os seguintes pré-requisitos foram atendidos:

- O usuário tem o direito de **Modificar ACLs de objetos** na área funcional **Recursos gerais: permissões do usuário**. Caso não tenha esse direito, a guia para configurar o modo estará ausente.
- O usuário tem o direito de **Leitura** na área funcional **Recursos gerais: funcionalidade básica**.

Caso uma hierarquia de Servidores de Administração esteja organizada em sua rede, para configurar o modo somente painel, acesse o servidor onde a conta de usuário está disponível na guia **Usuários** da seção **Usuários e funções → Usuários e grupos**. Pode ser um servidor principal ou um servidor secundário físico. Não é possível ajustar o modo em um servidor virtual.

Para configurar o modo somente painel:

1. No menu principal, vá para **Usuários e funções → Usuários e grupos** e selecione a guia **Usuários**.
2. Clique no nome da conta de usuário para a qual deseja ajustar o painel com widgets.
3. Na janela aberta de configurações do usuário, selecione a guia **Painel**.

   Na guia aberta, o mesmo painel é exibido para você e para o usuário.
4. Caso o **modo Exibir o console no modo somente painel** estiver habilitado, alterne o botão de alternância para desativá-la.

   Quando essa opção está habilitada, também não será possível alterar o painel. Depois de desativar a opção, será possível gerenciar widgets.
5. Configure a aparência do painel. O conjunto de widgets preparados na guia **Painel** está disponível para o usuário com a conta personalizável. Ele ou ela não pode alterar nenhuma configuração ou tamanho dos widgets, adicionar ou remover quaisquer widgets do painel. Portanto, ajuste-os para o usuário, para que ele possa visualizar as estatísticas de proteção da rede. Para isso, na guia **Painel** é possível executar as mesmas ações com widgets como na seção **Monitoramento e relatórios → Painel**:
   - Adicionar novos widgets ao painel.
   - Ocultar widgets que o usuário não precisa.
   - Mover widgets em uma ordem específica.
   - Alterar o tamanho ou a aparência de widgets.
   - Alterar as configurações do widget.
6. Alterne o botão de alternância para habilitar a opção **Exibir o console no modo somente painel**.

   Depois disso, apenas o painel ficará disponível para o usuário. Ele ou ela pode monitorar as estatísticas, mas não pode alterar as configurações de proteção de rede e a aparência do painel. Como o mesmo painel é exibido para você e para o usuário, você também não pode alterar o painel.

   Caso mantenha a opção desativada, o menu principal será exibido ao usuário, para que ele possa realizar várias ações no Kaspersky Security Center Cloud Console, inclusive alterar as configurações de segurança e os widgets.
7. Clique no botão **Salvar** quando terminar de configurar o modo somente painel. Somente depois disso o dashboard preparado será exibido ao usuário.
8. Caso o usuário queira visualizar as estatísticas de aplicativos Kaspersky compatíveis e precisar de direitos de acesso para isso, configure os direitos para o usuário. Depois disso, os dados dos aplicativos Kaspersky são exibidos para o usuário nos widgets desses aplicativos.

Agora, o usuário pode fazer login no Kaspersky Security Center Cloud Console com a conta personalizada e monitorar as estatísticas de proteção de rede no modo somente painel.

Relatórios

Esta seção descreve como usar relatórios, gerenciar modelos de relatórios personalizados, usar modelos de relatórios para gerar novos relatórios e criar tarefas de entrega de relatórios.

Usar os relatórios

O recurso Relatórios permite obter informações numéricas detalhadas sobre a segurança da rede da sua organização, salvar essas informações em um arquivo, enviá-las por e-mail e imprimi-las.

Os relatórios estão disponíveis no Kaspersky Security Center Cloud Console, na seção **Monitoramento e relatórios**, clicando em **Relatórios**.

Por padrão, os relatórios contém informações dos últimos 30 dias.

O Kaspersky Security Center Cloud Console tem um conjunto padrão de relatórios para as seguintes categorias:

- **Status da proteção**
- **Implementação**
- **Atualizando**
- **Estatísticas de ameaças**
- **Outro**

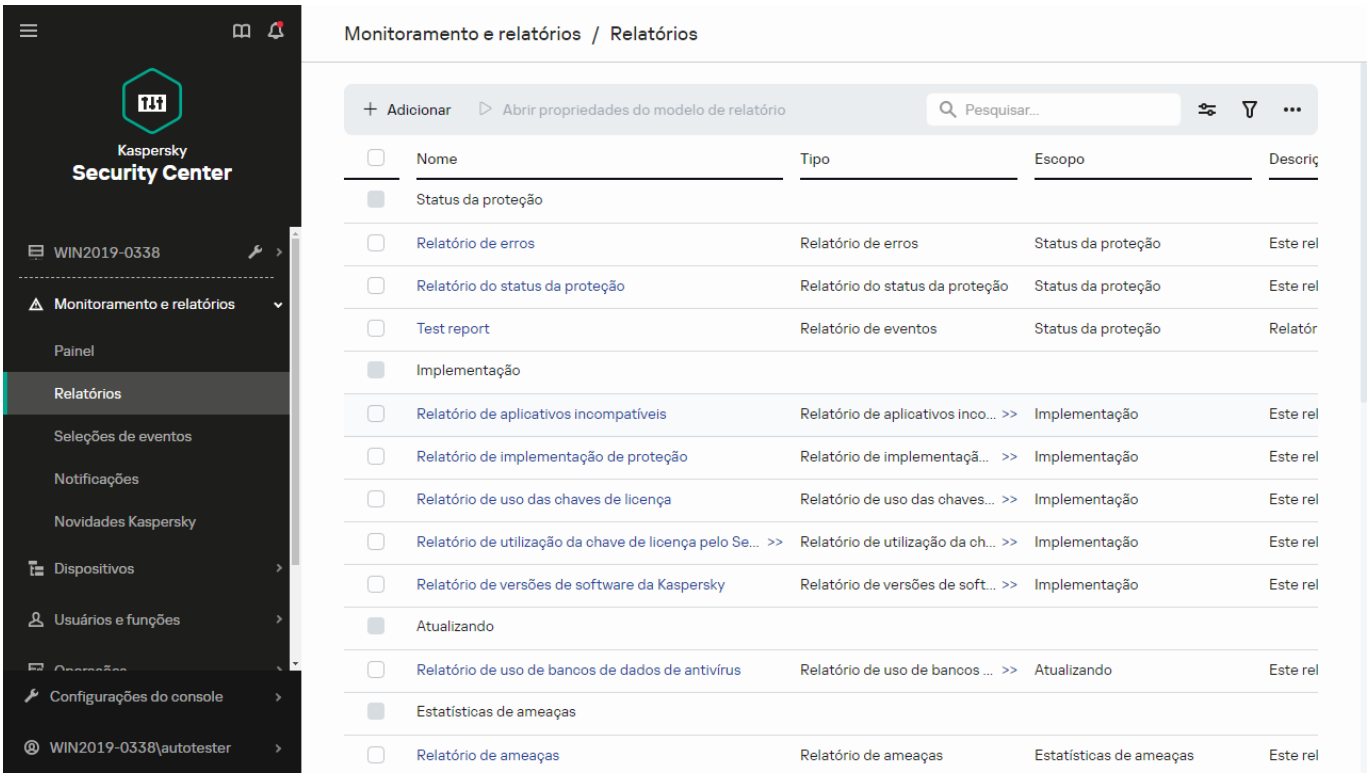
Você pode criar modelos de relatório personalizados, editar modelos de relatório e excluí-los.

Você pode criar relatórios que são baseados em modelos existentes, exportar relatórios para arquivos e criar tarefas para entrega de relatório.

Criação de um modelo de relatório

Para criar um modelo de relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.

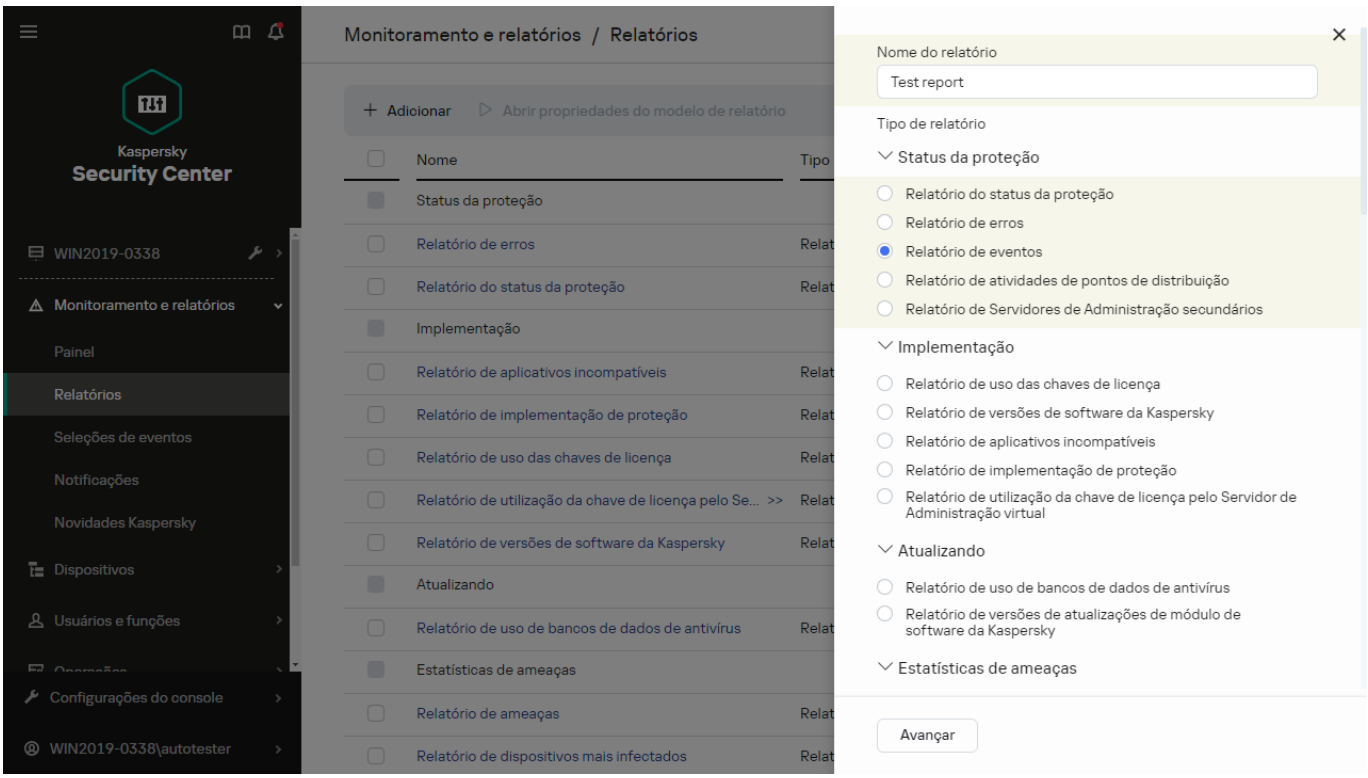


A lista dos modelos de relatório na subseção Relatórios

2. Clique em **Adicionar**.

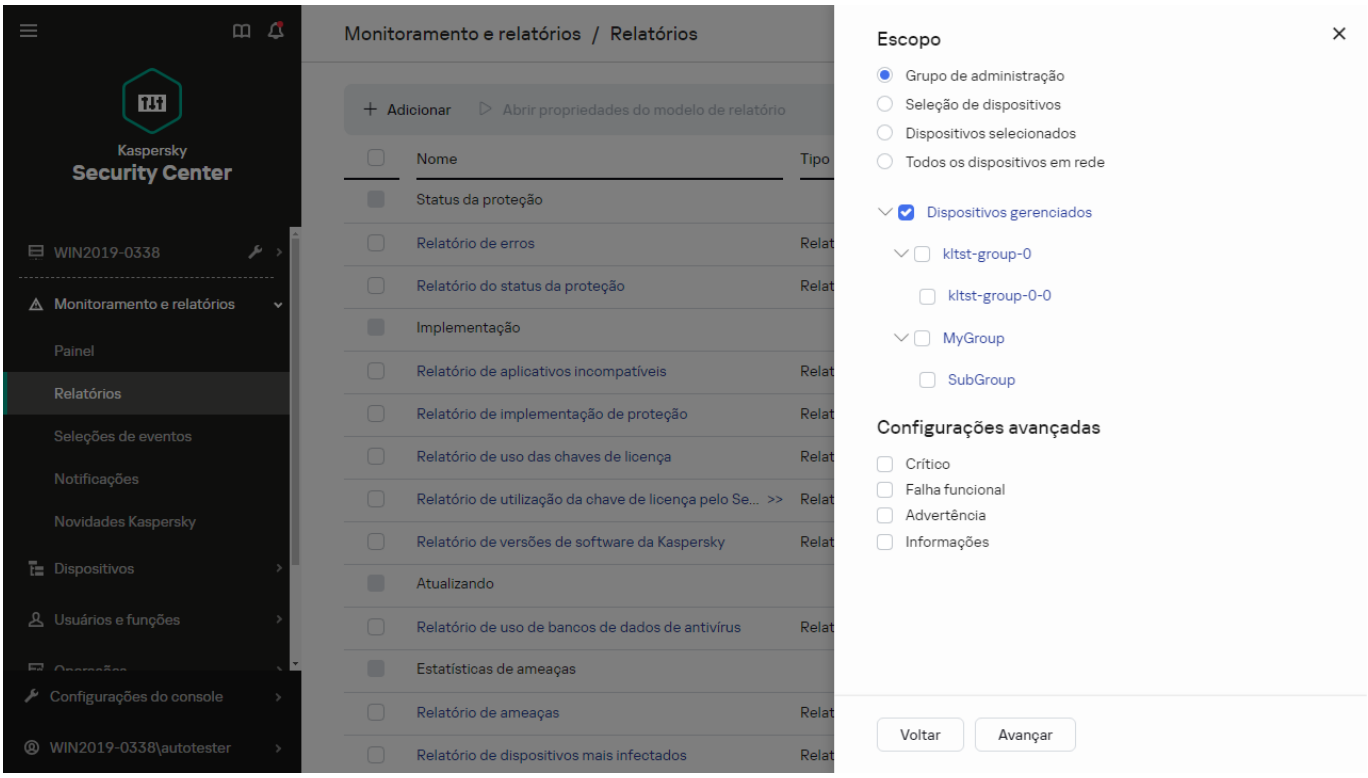
   O assistente de novo modelo de relatório é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

3. Na primeira página do assistente, digite o nome de relatório e selecione o tipo de relatório.



O assistente de Novo modelo de relatório. Especificar o nome e o tipo do modelo de relatório

4. Na página **Escopo** do assistente, selecione o conjunto de dispositivos cliente (grupo de administração, seleção de dispositivos, dispositivos selecionados ou todos os dispositivos em rede) cujos dados serão exibidos em relatórios que são baseados nesse modelo de relatório.

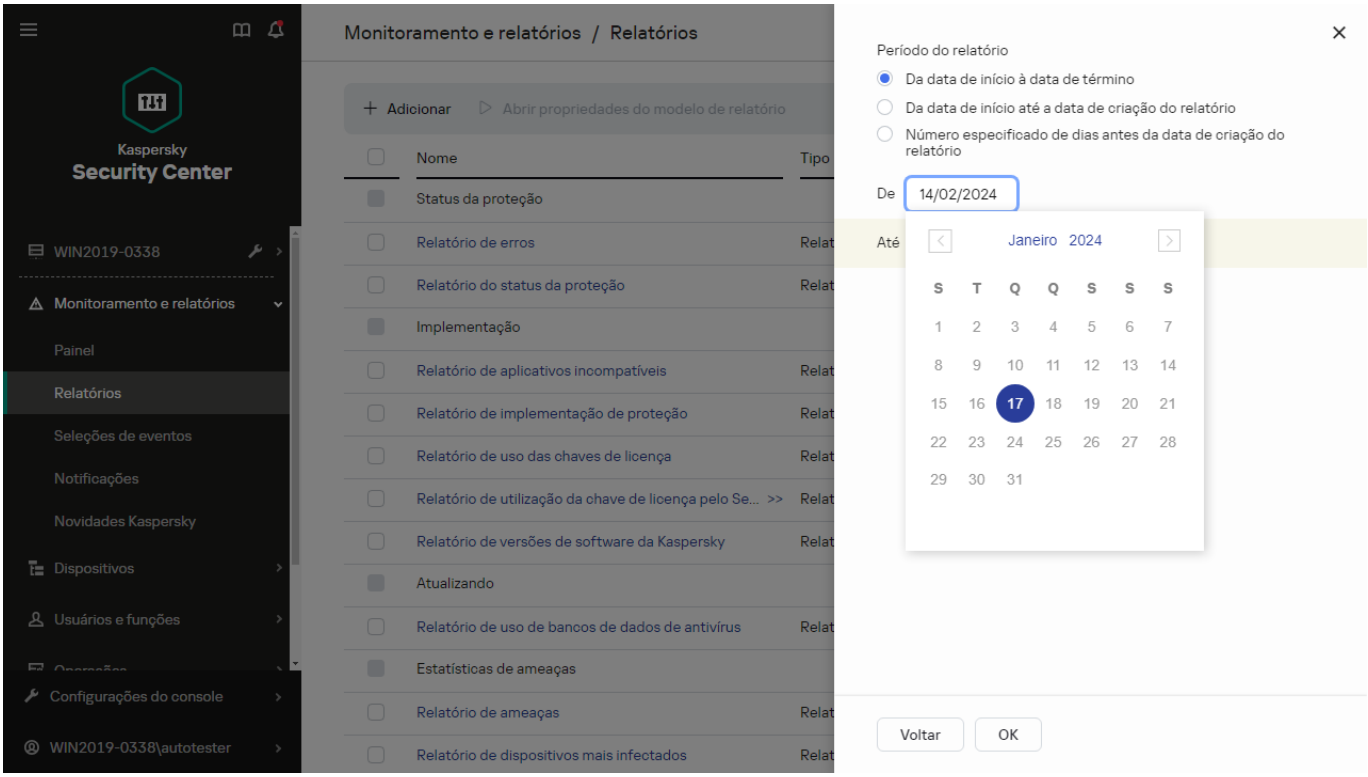


O assistente de Novo modelo de relatório. Especificar o escopo do modelo de relatório

5. Na página **Período do relatório** do assistente, especifique o período de relatório. Os valores disponíveis são:

   - Entre as duas datas especificadas
   - A partir da data especificada até à data de criação do relatório
   - Desde a data de criação do relatório menos o número especificado de dias, até a data de criação do relatório

   Essa página pode não aparecer para alguns relatórios.



O assistente de Novo modelo de relatório. Especificar o período do relatório

6. Clique em **OK** para fechar o assistente.

7. Execute uma das seguintes ações:

   - Clique no botão **Salvar e executar** para salvar o novo modelo de relatório e executar um relatório baseado nele.

     O modelo de relatório é salvo. O relatório é gerado.

   - Clique no botão **Salvar** para salvar o novo modelo de relatório.

     O modelo de relatório é salvo.

Você pode usar o novo modelo para gerar e visualizar relatórios.

Visualização e edição das propriedades do modelo de relatório

Você pode visualizar e editar propriedades básicas de um modelo de relatório como, por exemplo, o nome do modelo de relatório ou os campos exibidos no relatório.

Para visualizar e editar propriedades de um modelo de relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.

2. Marque a caixa de seleção ao lado do modelo de relatório cujas propriedades deseja visualizar e editar.

   Como uma alternativa, você pode primeiro gerar o relatório e depois clicar no botão **Editar**.

3. Clique no botão **Abrir propriedades do modelo de relatório**.

   A janela **Edição de relatório <Nome do relatório>** é exibida com a guia **Geral** selecionada.

4. Edite as propriedades do modelo de relatório:

   - Guia **Geral**:

     - Nome do modelo de relatório

     - **Número máximo de entradas a exibir**

Se esta opção estiver ativada, o número de entradas exibidas na tabela com dados de relatório detalhados não será maior que o valor especificado. Observe que esta opção não afeta o número máximo de eventos que é possível incluir no relatório ao exportar o relatório para um arquivo.

As entradas de relatório são primeiro classificadas segundo as regras especificadas na seção **Campos → Campos de detalhes** das propriedades do modelo de relatório e, em seguida, apenas a primeira das entradas resultantes é mantida. O cabeçalho da tabela com dados de relatório detalhados mostra o número de entradas exibidas e o número total de entradas disponíveis que combinam com outras configurações do modelo de relatório.

Se esta opção estiver desativada, a tabela com dados de relatório detalhados exibe todas as entradas disponíveis. Não recomendamos que você desative essa opção. Limitar o número de entradas de relatório exibidas reduz a carga do sistema de gerenciamento de banco de dados (DBMS) e reduz o tempo necessário para gerar e exportar o relatório. Alguns dos relatórios contêm entradas excessivas. Se este for o caso, você pode ter dificuldade para ler e analisar todas elas. Além disso, o seu dispositivo pode ficar sem memória ao gerar um relatório e, consequentemente, você não poderá exibir o relatório.

Por padrão, esta opção está ativada. O valor predefinido é de 1.000.

Observe que a interface do Kaspersky Security Center Cloud Console pode exibir no máximo 2500 entradas. Se precisar visualizar uma quantidade maior de eventos, use o recurso de exportação de relatório.

- **Grupo**

  Clique no botão **Configurações** para alterar o conjunto de dispositivos cliente para os quais o relatório é criado. Para alguns tipos dos relatórios, o botão pode estar indisponível. As configurações reais dependem das configurações especificadas durante a criação do modelo de relatório.

- **Intervalo de tempo**

  Clique no botão **Configurações** para modificar o período de relatório. Para alguns tipos dos relatórios, o botão pode estar indisponível. Os valores disponíveis são:

  - Entre as duas datas especificadas
  - A partir da data especificada até à data de criação do relatório
  - Desde a data de criação do relatório menos o número especificado de dias, até a data de criação do relatório

- **Incluir dados dos Servidores de Administração secundários e virtuais**

  Se esta opção estiver ativada, o relatório inclui as informações dos Servidores de Administração secundário e virtual subordinados ao Servidor de Administração para o qual o modelo de relatório é criado.

  Desative esta opção se você quiser visualizar dados somente do Servidor de Administração atual.

  Por padrão, esta opção está ativada.

- **Até o nível de aninhamento**

  O relatório inclui dados de servidores de administração secundários e virtuais localizados sob o Servidor de administração atual a um nível de agrupamento menor ou igual ao valor especificado.

  O valor padrão é 1. Convém alterar esse valor caso necessite recuperar as informações dos Servidores de administração secundários localizados em níveis mais baixos na árvore.

- Intervalo de espera dos dados (min.)

  Antes de gerar o relatório, o Servidor de administração para o qual o modelo de relatório é criado aguarda pelos dados de Servidores de administração secundários durante o número de minutos especificado. Se nenhum dado for recebido de um Servidor de administração secundário ao fim desse período, o relatório é executado mesmo assim. Em vez de dados reais, o relatório exibe os dados retirados do cache (se a opção **Dados em cache dos Servidores de Administração secundários** estiver ativada) ou, caso contrário, **N/A** (não acessível).

  O valor predefinido é de 5 (minutos).

- Dados em cache dos Servidores de Administração secundários

  Os Servidores de Administração secundários regularmente transferem dados para o Servidor de Administração para o qual o modelo de relatório é criado. Nesse local, os dados transferidos são armazenados em cache.

  Se o Servidor de administração atual não puder receber dados de um Servidor de administração secundário enquanto o relatório estiver sendo gerado, o relatório exibirá dados retirados do cache. A data em que os dados foram transferidos para o cache também é exibida.

  Ativar essa opção permite a visualização das informações dos Servidores de administração secundários, mesmo se os dados atualizados não puderem ser recuperados. Entretanto, os dados exibidos podem ser obsoletos.

  Por padrão, esta opção está desativada.

- Frequência de atualização de cache (h)

  Os Servidores de administração secundários regularmente transferem dados para o Servidor de administração para o qual o modelo de relatório é criado. É possível especificar o período em horas. Se o valor for 0, os dados serão transferidos somente quando o relatório for gerado.

  O valor padrão é 0.

- Transferir informações detalhadas dos Servidores de Administração secundários

  No relatório gerado, a tabela contendo dados de relatório detalhados inclui dados dos Servidores de Administração secundários do Servidor de Administração para o qual o modelo de relatório é criado.

  Ativar esta opção reduz a velocidade de geração de relatórios e aumenta o tráfego entre Servidores de Administração. Entretanto, você pode visualizar todos os dados em um relatório.

  Em vez de ativar a opção, convém analisar dados de relatório detalhados para detectar um Servidor de administração secundário defeituoso e, em seguida, gerar o mesmo relatório apenas para o Servidor de administração defeituoso.

  Por padrão, esta opção está desativada.

- Guia **Campos**

  Selecione os campos que serão exibidos no relatório e use os botões **Para cima** e **Para baixo** para alterar a ordem desses campos. Use o botão **Adicionar** ou **Editar** para especificar se as informações no relatório devem ser classificadas e filtradas segundo cada um dos campos.

Na seção **Filtros dos campos Detalhes**, você também pode clicar em **Converter filtros** para começar a usar o formato de filtragem estendido. Este formato permite combinar as condições de filtragem especificadas em vários campos, usando a operação lógica OR. Depois de clicar no botão, o painel **Converter filtros** abre à direita. Clique no botão **Converter filtros** para confirmar a conversão. Agora, você pode definir um filtro convertido com as condições da seção **Campos de detalhes**, que são aplicadas usando a operação lógica OR.

A conversão de um relatório para o formato compatível com as condições de filtragem complexas tornará o relatório incompatível com as versões anteriores do Kaspersky Security Center (11 e anteriores). Além disso, o relatório convertido não conterá nenhum dado dos Servidores de Administração secundários executando tais versões incompatíveis.

5. Clique em **Salvar** para salvar as alterações.

6. Feche a janela **Editar relatório <Nome do relatório>**.

O modelo de relatório atualizado aparece na lista de modelos de relatório.

Exportar um relatório para um arquivo

É possível salvar um ou vários relatórios em XML, HTML ou PDF. O Kaspersky Security Center Cloud Console permite exportar até 10 relatórios para arquivos do formato especificado ao mesmo tempo.

Para exportar um relatório para um arquivo:

1. No menu principal, vá para **Monitoramento e relatórios → Relatórios**.

2. Escolha os relatórios que deseja exportar.

   Caso queira escolher mais de 10 relatórios, o botão **Exportar relatório** será desativado.

3. Clique no botão **Exportar relatório**.

4. Na janela aberta, especifique os seguintes parâmetros de exportação:

   - **Nome de arquivo**.

     Ao selecionar um relatório para exportar, especifique o nome do arquivo do relatório.

     Ao selecionar mais de um relatório, os nomes dos arquivos de relatório coincidirão com o nome dos modelos de relatório selecionados.

   - **Número máximo de entradas**.

     Especifique o número máximo de entradas incluídas no arquivo de relatório. O valor padrão é 10.000.

   - **Formato do arquivo**.

     Selecione o tipo de arquivo do relatório: XML, HTML ou PDF. Ao exportar vários relatórios, todos os relatórios selecionados serão salvos no formato especificado como arquivos separados.

5. Clique no botão **Exportar relatório**.

O relatório é salvo em um arquivo no formato especificado.

Como gerar e visualizar um relatório

Para criar e visualizar um relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. Clique no nome do modelo de relatório que deseja usar para criar um relatório.

Um relatório usando o modelo selecionado é gerado e exibido.

Os dados do relatório são exibidos apenas em inglês, outros idiomas não estão disponíveis.

O relatório exibe os seguintes dados:

- Na guia **Resumo**:
  - O nome e tipo de relatórios, uma breve descrição e o período de relatórios, assim como as informações sobre o grupo de dispositivos para os quais o relatório é gerado.
  - Gráfico que mostra os dados do relatório mais representativos.
  - Tabela consolidada com os indicadores do relatório calculados.
- Na guia **Detalhes**, uma tabela com dados detalhados do relatório é exibida.

Criação de uma tarefa de entrega de relatório

Você pode criar uma tarefa que entregará os relatórios selecionados.

Para criar uma tarefa de entrega de um relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. [Opcional] Marque as caixas de seleção ao lado dos modelos de relatório para os quais deseja criar uma tarefa de entrega de relatório.
3. Clique no botão **Nova tarefa de entrega de relatórios**.
4. O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
5. Na primeira página do assistente, digite o nome da tarefa. O nome padrão é **Entregar relatórios (<N>)**, em que <N> é o número de sequência da tarefa.
6. Na página de configurações da tarefa do assistente, especifique as seguintes configurações:
   a. Modelos de relatório a serem entregues pela tarefa. Caso os tenha selecionado na etapa 2, ignore esta etapa.
   b. O formato do relatório: HTML, XLS ou PDF.

c. Se os relatórios precisarem ser enviados por e-mail, em conjunto com as configurações de notificação por e-mail.

7. Se você deseja modificar outras configurações de tarefa após a criação da tarefa, na página **Concluir a criação da tarefa** do assistente, habilite a opção **Abrir detalhes da tarefa quando a criação for concluída**.

8. Clique no botão **Criar** para criar a tarefa e fechar o assistente.

   A tarefa de entrega de relatório é criada. Se você ativou a opção **Abrir detalhes da tarefa quando a criação for concluída**, a janela de configurações da tarefa é aberta.

Excluir os modelos de relatório

Para excluir um ou vários modelos de relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.

2. Marque as caixas de seleção ao lado dos modelos de relatório que deseja excluir.

3. Clique no botão **Excluir**.

4. Na janela que se abre, clique em **OK** para confirmar a sua seleção.

Os modelos de relatório selecionados são excluídos. Se esses modelos de relatório tiverem sido incluídos nas tarefas de entrega de relatório, eles também serão removidos das tarefas.

Eventos e seleções de eventos

Esta seção fornece informações sobre eventos e seleções de eventos, sobre os tipos de eventos que ocorrem nos componentes do Kaspersky Security Center Cloud Console e sobre como gerenciar o bloqueio de eventos frequentes.

Sobre eventos no Kaspersky Security Center Cloud Console

O Kaspersky Security Center Cloud Console lhe permite receber informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nestes dispositivos gerenciados. As informações sobre eventos são salvas no banco de dados do Servidor de Administração. É possível exportar estas informações para sistemas SIEM externos. Exportar informações sobre o evento aos sistemas SIEM externos permite que os administradores de sistemas SIEM respondam prontamente aos eventos de sistema de segurança que ocorrem em dispositivos gerenciados ou em grupos de dispositivos.

Eventos por tipo

No Kaspersky Security Center Cloud Console, há os seguintes tipos de eventos:

- Eventos gerais. Esses eventos ocorrem em todos os aplicativos Kaspersky gerenciados. Um exemplo de um evento geral é um Surto de vírus. Eventos gerais têm sintaxe e semântica estritamente definidas. Eventos gerais são usados, por exemplo, em relatórios e painéis.

- Eventos gerenciados específicos de aplicativos Kaspersky. Cada aplicativo Kaspersky gerenciado tem o seu próprio conjunto de eventos.

Eventos por origem

É possível ver a lista completa dos eventos que podem ser gerados por um aplicativo na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar a lista de eventos nas propriedades do Servidor de Administração.

Os eventos podem ser gerados pelos seguintes aplicativos:

- Componentes do Kaspersky Security Center Cloud Console:
  - Servidor de Administração
  - Agente de Rede
- Aplicativos gerenciados pela Kaspersky

  Para obter detalhes sobre os eventos gerados pelos aplicativos gerenciados pela Kaspersky, consulte a documentação do aplicativo correspondente.

Eventos por nível de importância

Cada evento tem o seu próprio nível de importância. Dependendo das condições da sua ocorrência, a um evento pode ser atribuídos diversos níveis de importância. Há quatro níveis de importância de eventos:

- Um *evento crítico* é um evento que indica a ocorrência de um problema crítico que pode levar à perda de dados, um funcionamento operacional ruim ou um erro crítico.
- Uma *falha funcional* é um evento que indica a ocorrência de um problema sério, erro ou funcionamento incorreto que ocorreu durante a operação do aplicativo ou ao executar um procedimento.
- Um *aviso* é um evento que não necessariamente é sério, mas no entanto indica um problema potencial no futuro. A maior parte de eventos são indicados como avisos se o aplicativo puder ser restaurado sem perda dos dados ou capacidades funcionais após a ocorrência de tais eventos.
- Um evento *de informação* é um evento que ocorre para fins de informar sobre conclusão bem sucedida de uma operação, funcionamento apropriado do aplicativo ou conclusão de um procedimento.

Cada evento tem um prazo de armazenamento definido, durante o qual você pode exibi-lo ou modificá-lo no Kaspersky Security Center Cloud Console. Alguns eventos não são salvos no banco de dados do Servidor de Administração por padrão porque o seu prazo de armazenamento definido é zero. Somente os eventos que serão armazenados no banco de dados do Servidor de Administração por ao menos um dia podem ser exportados aos sistemas externos.

Eventos dos componentes do Kaspersky Security Center Cloud Console

Cada componente do Kaspersky Security Center Cloud Console tem o seu próprio conjunto de tipos de evento. Esta seção lista tipos de eventos que ocorrem no Servidor de Administração e no Agente de Rede do Kaspersky Security Center Cloud Console. Os tipos de eventos que ocorrem nos aplicativos Kaspersky não são listados nesta seção.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Estrutura de dados da descrição do tipo de evento

Para cada tipo de evento, seu nome de exibição, o identificador (ID), o código alfabético, a descrição e o termo de armazenamento padrão são fornecidos.

- **Nome de exibição do tipo de evento**. Este texto é exibido no Kaspersky Security Center Cloud Console quando você configura eventos e quando eles ocorrem.
- **ID do tipo de evento**. Este código numérico é usado quando você processa eventos usando ferramentas de terceiros para a análise de eventos.
- **Tipo de evento** (código alfabético). Este código é usado quando você percorre e processa eventos usando visualizações públicas fornecidas no banco de dados do Kaspersky Security Center Cloud Console.
- **Descrição**. Este texto contém as situações nas quais um evento ocorre e o que você pode fazer nesses casos.
- **Prazo de armazenamento padrão**. É o número de dias durante os quais o evento é armazenado no banco de dados do Servidor de Administração e é exibido na lista de eventos no Servidor de Administração. Após o término desse período, o evento é excluído. Se o valor do prazo de armazenamento do evento for 0, os eventos são detectados, mas não são exibidos na lista de eventos no Servidor de Administração.

Eventos do Servidor de Administração

Esta seção contém informações sobre os eventos relativos ao Servidor de Administração.

Eventos críticos do Servidor de Administração

A tabela abaixo exibe os eventos do servidor de administração do Kaspersky Security Center Cloud Console com o nível de importância **Crítico**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos críticos do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo armazenar padrã
O limite da licença foi excedido	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Uma vez por dia o Kaspersky Security Center Cloud Console verifica se a restrição de	180 dias

			licenciamento foi excedida. Eventos deste tipo ocorrem quando Servidor de Administração detectar que alguns limites de licenciamento estão excedidos pelos aplicativos da Kaspersky instalados nos dispositivos cliente e se o número de unidades de licenciamento atualmente usadas e cobertas por uma única licença exceder 110% do número total de unidades cobertas pela licença. Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua os dispositivos que não estão em uso. • Forneça uma licença para mais dispositivos (adicione um código de ativação ou arquivo de chave válido no Servidor de Administração).

			O Kaspersky Security Center Cloud Console determina as regras para gerar eventos quando uma restrição de licenciamento for excedida.	
Surto de vírus	26 (para Proteção Contra Ameaças ao Arquivo)	GNRL_EV_VIRUS_OUTBREAK	Eventos deste tipo ocorrem quando o número de objetos maliciosos detectados em diversos dispositivos gerenciados exceder o limite dentro de um curto período de tempo. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o limite nas propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	180 dias
Surto de vírus	27 (para Proteção Contra Ameaças ao Correio)	GNRL_EV_VIRUS_OUTBREAK	Eventos deste tipo ocorrem quando o número de objetos maliciosos detectados em diversos dispositivos gerenciados exceder o limite dentro de um curto período de tempo. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o	180 dias

			limite nas propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	
Surto de vírus	28 (para Firewall)	GNRL_EV_VIRUS_OUTBREAK	Eventos deste tipo ocorrem quando o número de objetos maliciosos detectados em diversos dispositivos gerenciados exceder o limite dentro de um curto período de tempo. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o limite nas propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	180 dias
O dispositivo está sem gerenciamento	4111	KLSRV_HOST_OUT_CONTROL	Eventos deste tipo ocorrem se um dispositivo gerenciado está visível na rede, mas não se conectou ao Servidor de Administração por	180 dias

			um período de tempo específico. Descubra o que impede o funcionamento apropriado do Agente de Rede no dispositivo. As causas possíveis incluem problemas de rede e a remoção do Agente de Rede do dispositivo.	
O status do dispositivo é Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	Eventos deste tipo ocorrem quando um dispositivo gerenciado é atribuído com o status *Crítico*. Você pode configurar as condições sob as quais o status do dispositivo é alterado para *Crítico*.	180 dias
Modo de funcionalidade limitada	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Eventos desse tipo ocorrem quando o Kaspersky Security Center Cloud Console inicia a operação com a funcionalidade básica, sem o Gerenciamento de patches e vulnerabilidades e sem os recursos de Gerenciamento de Dispositivos Móveis. A seguir se encontram as causas de, e as respostas apropriadas, do evento: • Termo da licença expirado. Forneça uma licença para usar a funcionalidade completa do Kaspersky Security Center Cloud Console (adicione um código de ativação ou um arquivo de chave	180 dias

			válido no Servidor de Administração). • O Servidor de Administração gerencia mais dispositivos do que o especificado pelo limite da licença. Mover dispositivos dos grupos de administração de um Servidor de Administração para aqueles de outro Servidor (se o limite da licença do outro Servidor de Administração o permitir).	
A licença expira em breve	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Eventos desse tipo ocorrem quando a data de expiração da licença comercial está se aproximando. Uma vez ao dia, o Kaspersky Security Center verifica se a data de expiração da licença está próxima. Eventos deste tipo são publicados 30 dias, 15 dias, 5 dias e 1 dia antes da data de expiração da licença. Este número de dias não pode ser alterado. Se o Servidor de Administração é desativado no dia especificado antes da data de expiração da licença, o evento não será publicado até o próximo dia.	180 dias

			Quando a licença comercial expirar, o Kaspersky Security Center Cloud Console fornecerá apenas a funcionalidade básica. Você pode responder ao evento nas seguintes maneiras: • Certifique-se de que uma chave reserva de licença seja adicionada ao Servidor de Administração. • Caso use uma assinatura, certifique-se de renová-la. Uma assinatura ilimitada será automaticamente renovada, caso tenha sido pré-paga ao provedor de serviços na data devida.	
O certificado expirou	4132	KLSRV_CERTIFICATE_EXPIRED	As informações serão adicionadas em breve.	180 dias
As atualizações dos módulos de software da Kaspersky foram revogadas	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Eventos deste tipo ocorrem se as atualizações racionais tenham sido revogadas (o status *Revogada* é exibido para essas atualizações) pelos especialistas técnicos da Kaspersky; por exemplo, elas precisam ser atualizadas para uma versão mais nova. Este evento é relativo às correções do Kaspersky Security Center Cloud Console e não relativos aos	180 dias

			módulos dos aplicativos gerenciados da Kaspersky. O evento fornece o motivo da não instalação das atualizações racionais.	
Auditoria: falha na exportação para SIEM	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Eventos desse tipo ocorrem quando a exportação de eventos para o sistema SIEM falha devido a um erro de conexão com o sistema SIEM.	180 dias

Eventos de falha funcional do Servidor de Administração

A tabela abaixo mostra os eventos do servidor de administração do Kaspersky Security Center Cloud Console com o nível de importância **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O limite de instalações foi excedido para um dos grupos de aplicativos licenciados	4126	KLSRV_INVLICPROD_EXCEDED	O Servidor de Administração gera periodicamente eventos deste tipo (a cada hora). Eventos deste tipo ocorrem se no Kaspersky Security Center Cloud Console você gerencia chaves de licença de aplicativos de terceiros e o número de instalações excedeu o limite definido pela chave de licença do aplicativo de terceiro. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua o aplicativo de terceiro dos dispositivos nos quais o aplicativo não está em uso.	180 dias

			• Use uma licença de terceiro para mais dispositivos. Você pode gerenciar chaves de licença de aplicativos de terceiros usando a funcionalidade de grupos de aplicativos licenciados. Um grupo de aplicativos licenciados inclui aplicativos de terceiros que atendem os critérios definidos por você.	

Eventos de aviso do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração do Kaspersky Security Center Cloud Console com o nível de importância **Advertência**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de aviso do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamen padrão
O limite da licença foi excedido	4098	KLSRV_EV_LICENSE_CHECK_100_110	Uma vez por dia o Kaspersky Security Center Cloud Console verifica se a restrição de licenciamento foi excedida.	90 dias

				Eventos deste tipo ocorrem quando Servidor de Administração detectar que alguns limites de licenciamento estão excedidos pelos aplicativos da Kaspersky instalados nos dispositivos cliente e se o número de unidades de licenciamento atualmente usadas e cobertas por uma única licença exceder 100% a 110% do número total de unidades cobertas pela licença. Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua os dispositivos que não estão em uso. • Forneça uma licença para mais dispositivos (adicione um código de ativação ou arquivo de chave válido no Servidor de Administração).

			O Kaspersky Security Center Cloud Console determina as regras para gerar eventos quando uma restrição de licenciamento for excedida.	
O dispositivo permaneceu inativo na rede por muito tempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	As informações serão adicionadas em breve.	90 dias
Conflito de nomes de dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	As informações serão adicionadas em breve.	90 dias
O status do dispositivo é Advertência	4114	KLSRV_HOST_STATUS_WARNING	Eventos deste tipo ocorrem quando à um dispositivo gerenciado for atribuído o status de *Aviso*. Você pode configurar as condições sob as quais o status do dispositivo é alterado para *Aviso*.	90 dias
O limite de instalações será atingido para um dos grupos de aplicativos licenciados	4127	KLSRV_INVLICPROD_FILLED	As informações serão adicionadas em breve.	90 dias
O certificado foi solicitado	4133	KLSRV_CERTIFICATE_REQUESTED	As informações serão adicionadas em breve.	90 dias
O certificado foi removido	4134	KLSRV_CERTIFICATE_REMOVED	As informações serão adicionadas em breve.	90 dias
O certificado de APNs expirou	4135	KLSRV_APN_CERTIFICATE_EXPIRED	As informações serão adicionadas em breve.	90 dias
O certificado de APNs expira em breve	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	As informações serão adicionadas em breve.	90 dias
Falha ao enviar	4138	KLSRV_GCM_DEVICE_ERROR	As informações	90 dias

a mensagem FCM para o dispositivo móvel			serão adicionadas em breve.	
Ocorreu um erro de HTTP ao enviar a mensagem FCM para o servidor FCM	4139	KLSRV_GCM_HTTP_ERROR	As informações serão adicionadas em breve.	90 dias
Falha ao enviar a mensagem FCM para o servidor FCM	4140	KLSRV_GCM_GENERAL_ERROR	As informações serão adicionadas em breve.	90 dias
A conexão com o Servidor de Administração secundário foi interrompida	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	As informações serão adicionadas em breve.	90 dias
A conexão com o Servidor de Administração principal foi interrompida	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	As informações serão adicionadas em breve.	90 dias
Proxy da KSN iniciado. Falha ao verificar a disponibilidade da KSN	7719	KSNPROXY_STARTED_CON_CHK_FAILED	As informações serão adicionadas em breve.	90 dias
Novas atualizações para os módulos de software da Kaspersky foram registradas	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	As informações serão adicionadas em breve.	90 dias
O limite de eventos no banco de dados foi excedido. A exclusão dos eventos foi iniciada	4145	KLSRV_EVP_DB_TRUNCATING	Eventos deste tipo ocorrem quando a exclusão de eventos antigos do banco de dados do Servidor de Administração começou após a capacidade do banco de dados do Servidor de Administração ter sido alcançada.	90 dias

			Você pode responder ao evento nas seguintes maneiras: • Alterar o número máximo de eventos armazenados no banco de dados do servidor de administração. • Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração.	
O limite de eventos no banco de dados foi excedido. Os eventos foram excluídos	4146	KLSRV_EVP_DB_TRUNCATED	Eventos deste tipo ocorrem quando a exclusão de eventos antigos do banco de dados do Servidor de Administração começou após a capacidade do banco de dados do Servidor de Administração ter sido alcançada. Você pode responder ao evento nas seguintes maneiras: • Alterar o número máximo de eventos armazenados permitidos no banco de dados do servidor de administração. • Reduza a lista de eventos a serem armazenados	90 dias

			no banco de dados do Servidor de Administração.	
A licença expira em breve	4128	KLSRV_INVLICPROD_EXPIRED_SOON	As informações serão adicionadas em breve.	90 dias
Auditoria: falha no teste de conexão com o servidor SIEM	5120	KLAUD_EV_SIEM_TEST_FAILED	Eventos desse tipo ocorrem quando um teste de conexão automática com o servidor SIEM falha.	90 dias

Eventos informativos do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração do Kaspersky Security Center Cloud Console com o nível de importância **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Mais de 90% desta chave de licença foram utilizados	4097	KLSRV_EV_LICENSE_CHECK_90	30 dias
Novo dispositivo detectado	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 dias
O dispositivo foi migrado automaticamente de acordo com uma regra	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 dias
O dispositivo foi removido do grupo: inativo na rede por muito tempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 dias
O limite de instalações está prestes a ser excedido (mais de 95% já foram utilizados) para um dos grupos de aplicativos licenciados	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 dias
Foram encontrados arquivos para enviar para a Kaspersky para análise	4131	KLSRV_APS_FILE_APPEARED	30 dias
A ID da Instância FCM foi alterada neste dispositivo móvel	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 dias

As atualizações foram copiadas com êxito para a pasta especificada	4122	KLSRV_UPD_REPL_OK	30 dias
A conexão com o Servidor de Administração secundário foi estabelecida	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 dias
A conexão com o Servidor de Administração principal foi estabelecida	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 dias
Os bancos de dados foram atualizados (No Kaspersky Security Center Cloud Console, este tipo de evento somente está disponível para um Servidor de Administração secundário).	4144	KLSRV_UPD_BASES_UPDATED	30 dias
Proxy da KSN iniciado. A verificação de disponibilidade da KSN foi concluída com êxito	7718	KSNPROXY_STARTED_CON_CHK_OK	30 dias
Proxy da KSN parado	7720	KSNPROXY_STOPPED	30 dias
Auditoria: a conexão com o Servidor de Administração foi estabelecida	4147	KLAUD_EV_SERVERCONNECT	30 dias
Auditoria: o objeto foi modificado	4148	KLAUD_EV_OBJECTMODIFY	30 dias
Auditoria: o status do objeto foi alterado	4150	KLAUD_EV_TASK_STATE_CHANGED	30 dias
Auditoria: as configurações do grupo foram modificadas	4149	KLAUD_EV_ADMGROUP_CHANGED	30 dias
Auditoria: as chaves de criptografia foram importadas ou exportadas do Servidor de Administração	5100	KLAUD_EV_DPEKEYSEXPORT	30 dias
Auditoria: teste de conexão bem-sucedido com o servidor SIEM	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 dias

Eventos do Agente de Rede

Esta seção contém informações sobre os eventos relativos ao Agente de Rede.

Eventos de falha funcional do Agente de Rede

A tabela abaixo mostra os eventos do Agente de Rede do Kaspersky Security Center que têm o nível de gravidade **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Erro de instalação da atualização	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Eventos deste tipo ocorrem se a atualização e aplicação de patches automática para os componentes do Kaspersky Security Center Cloud Console forrem mal sucedidos. O evento não contém atualizações dos aplicativos gerenciados da Kaspersky. Leia a descrição do evento. Um problema do Windows no Servidor de Administração poderá ser o motivo desse evento. Se descrição mencionar qualquer problema da configuração do Windows, solucione o problema.	30 dias
Falha ao instalar a atualização de software de terceiros	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Eventos desse tipo ocorrem se os recursos de Gerenciamento de patches e vulnerabilidades e Gerenciamento de Dispositivos Móveis estiverem em uso e se a atualização do software de terceiros não tiver êxito.	30 dias

			Verificar se o link para o software de terceiros é válido. Leia a descrição do evento.	
Falha ao instalar as atualizações do Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Eventos deste tipo ocorrem se a atualizações do Windows não tiverem êxito. Configurar as atualizações do Windows em uma política de Agente de Rede. Leia a descrição do evento. Procure o erro na Base de Dados de Conhecimento da Microsoft. Entre em contato com o Suporte Técnico da Microsoft se você não conseguir resolver o problema você mesmo.	30 dias

Eventos de aviso do Agente de Rede

A tabela abaixo mostra os eventos do Agente de Rede do Kaspersky Security Center que têm o nível de gravidade **Advertência**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de aviso do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Uma advertência foi retornada durante a instalação da atualização dos módulos de software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 dias
A instalação da atualização do software de terceiros foi concluída com uma advertência	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 dias
A instalação da atualização do software de terceiros foi adiada	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 dias

Ocorreu um problema de segurança	549	GNRL_EV_APP_INCIDENT_OCCURED	30 dias
Proxy da KSN iniciado. Falha ao verificar a disponibilidade da KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 dias

Eventos informativos do Agente de Rede

A tabela abaixo mostra os eventos do Agente de Rede do Kaspersky Security Center que têm o nível de gravidade **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão
A atualização dos módulos de software foi instalada com êxito	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 dias
A instalação da atualização dos módulos de software começou	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 dias
Aplicativo instalado	7703	KLNAG_EV_INV_APP_INSTALLED	30 dias
Aplicativo desinstalado	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 dias
O aplicativo monitorado foi instalado	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 dias
O aplicativo monitorado foi desinstalado	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 dias
O aplicativo de terceiros foi instalado	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 dias
Novo dispositivo adicionado	7708	KLNAG_EV_DEVICE_ARRIVAL	30 dias
Dispositivo removido	7709	KLNAG_EV_DEVICE_REMOVE	30 dias
O dispositivo foi detectado	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dias
O dispositivo foi autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 dias

Windows Desktop Sharing: o arquivo foi lido	7712	KLUSRLOG_EV_FILE_READ	30 dias
Windows Desktop Sharing: o arquivo foi modificado	7713	KLUSRLOG_EV_FILE_MODIFIED	30 dias
Windows Desktop Sharing: aplicativo iniciado	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 dias
Windows Desktop Sharing: iniciado	7715	KLUSRLOG_EV_WDS_BEGIN	30 dias
Windows Desktop Sharing: parado	7716	KLUSRLOG_EV_WDS_END	30 dias
A atualização do software de terceiros foi instalada com êxito	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 dias
A instalação da atualização de software de terceiros foi iniciada	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 dias
Proxy da KSN iniciado. A verificação de disponibilidade da KSN foi concluída com êxito	7719	KSNPROXY_STARTED_CON_CHK_OK	30 dias
Proxy da KSN parado	7720	KSNPROXY_STOPPED	30 dias

Usar as seleções de eventos

As seleções de evento fornecem uma visualização na tela de conjuntos nomeados de eventos selecionados do banco de dados do Servidor de Administração. Esses conjuntos de eventos são agrupados de acordo com as seguintes categorias:

- Por nível de importância – **Eventos críticos**, **Falhas funcionais**, **Advertências** e **Eventos de informações**
- Por tempo – **Eventos recentes**
- Por tipo – **Pedidos de usuário** e **Eventos de auditoria**

Você pode criar e visualizar seleções de eventos definidos por usuários, com base nas configurações disponíveis, na interface do Kaspersky Security Center Cloud Console.

As seleções de eventos estão disponíveis no Kaspersky Security Center Cloud Console, na seção **Monitoramento e relatórios**, clicando em **Seleções de eventos**.

Por padrão, as seleções de eventos incluem informações dos últimos sete dias.

O Kaspersky Security Center Cloud Console tem um conjunto padrão de seleções de eventos (predefinidas):

- Eventos com níveis de importância diferentes:
  - **Eventos críticos**
  - **Falhas funcionais**
  - **Advertências**
  - **Mensagens informativas**
- **Solicitações de usuário** (eventos de aplicativos gerenciados)
- **Eventos recentes** (na semana passada)
- Eventos de auditoria

  No Kaspersky Security Center Cloud Console, os eventos de auditoria relacionados às operações de serviço no seu espaço de trabalho são exibidos. Esses eventos são condicionados por ações de especialistas da Kaspersky. Esses eventos, por exemplo, incluem o seguinte: Portas do Servidor de Administração mudando; Backup do banco de dados do Servidor de Administração; criação, modificação e exclusão de contas de usuário.

Você também pode criar e configurar seleções adicionais definidos pelo usuário. Em seleções definidas pelos usuários, é possível filtrar eventos pelas propriedades dos dispositivos dos quais se originaram (nomes de dispositivos, conjuntos de IPs e grupos de administração), por tipos de evento e níveis de gravidade, por aplicativo e nome do componente e por intervalo de tempo. Também é possível incluir resultados da tarefa no escopo de pesquisa. Você também pode usar um campo de pesquisa simples em que uma palavra ou várias palavras podem ser digitadas. São exibidos todos os eventos que contêm alguma das palavras digitadas em qualquer lugar nos seus atributos (como nome do evento, descrição, nome do componente).

Para seleções predefinidas e definidas pelos usuários, você pode limitar o número de eventos exibidos ou o número de registros para pesquisar. Ambas as opções afetam o tempo necessário para o Kaspersky Security Center Cloud Console exibir os eventos. Quanto maior for o banco de dados, mais demorado será o processo.

Você pode fazer o seguinte:

- Editar propriedades das seleções de eventos
- Gerar seleções de eventos
- Visualizar detalhes das seleções de eventos
- Excluir seleções de eventos
- Excluir eventos do banco de dados do Servidor de Administração

Criar uma seleção de eventos

Para criar uma seleção de eventos:

1. No menu principal, vá para **Monitoramento e relatórios** → **Seleções de eventos**.

2. Clique em **Adicionar**.

3. Na janela **Nova seleção de eventos** que se abre, especifique as configurações da nova seleção de eventos. Faça isso em uma ou mais das seções na janela.

4. Clique em **Salvar** para salvar as alterações.

   A janela de confirmação é exibida.

5. Para visualizar o resultado da seleção de eventos, mantenha a caixa de seleção **Ir para o resultado da seleção** selecionada.

6. Clique em **Salvar** para confirmar a criação da seleção de eventos.

Se você tiver mantido a caixa de seleção **Ir para o resultado da seleção** selecionada, o resultado da seleção de eventos será exibido. Caso contrário, a nova seleção de eventos será exibida na lista de seleção de eventos.

Editar uma seleção de eventos

Para editar uma seleção de eventos:

1. No menu principal, acesse **Monitoramento e relatórios** → **Seleções de eventos**.

2. Marque a caixa de seleção ao lado da seleção de eventos que deseja editar.

3. Clique no botão **Propriedades**.

   Uma janela de configurações de seleção de eventos é aberta.

4. Edite as propriedades da seleção de eventos.

   > Para seleções de eventos predefinidas, você pode editar somente as propriedades nas seguintes guias: **Geral** (exceto o nome de seleção), **Hora** e **Direitos de acesso**.

   Para seleções definidas pelos usuários, você pode editar todas as propriedades.

5. Clique em **Salvar** para salvar as alterações.

A seleção de eventos editada é mostrada na lista.

Visualizando uma lista de uma seleção de eventos

Para visualizar a seleção de eventos:

1. No menu principal, acesse **Monitoramento e relatórios** → **Seleções de eventos**.

2. Marque a caixa de seleção ao lado da seleção de eventos que deseja iniciar.

3. Execute uma das seguintes ações:

- Se você quiser configurar a classificação no resultado da seleção de eventos, faça o seguinte:

  a. Clique no botão **Reconfigurar classificação e iniciar**.

  b. Na janela exibida **Reconfigurar classificação para seleção de eventos**, especifique as configurações de classificação.

  c. Clique no nome da seleção.

- Caso contrário, se você quiser visualizar a lista de eventos e como eles estão classificados no Servidor de Administração, clique no nome da seleção.

O resultado da seleção de eventos é exibido.

Exportar uma seleção de eventos

O Kaspersky Security Center Cloud Console permite salvar uma seleção de evento e suas configurações em um arquivo KLO. É possível usar esse arquivo KLO para importar a seleção de eventos salva para o Kaspersky Security Center Windows e para o Kaspersky Security Center Linux.

Observe que é possível exportar apenas as seleções de eventos definidas pelo usuário. As seleções de eventos do conjunto padrão do Kaspersky Security Center Cloud Console (seleções predefinidas) não podem ser salvas em um arquivo.

Para exportar a seleção de eventos:

1. No menu principal, acesse **Monitoramento e relatórios → Seleções de eventos**.
2. Marque a caixa de seleção ao lado da seleção de eventos você deseja iniciar.

   Não é possível exportar as várias seleções de eventos ao mesmo tempo. Caso selecione mais de uma tarefa, o botão **Exportar** será desabilitado.
3. Clique no botão **Exportar**.
4. Na janela aberta **Salvar como**, especifique o nome e o caminho do arquivo de seleção de eventos e clique no botão **Salvar**.

   A janela **Salvar como** é exibida apenas se você usar Google Chrome, Microsoft Edge ou Opera. Caso outro navegador seja usado, o arquivo de seleção de eventos será salvo automaticamente na pasta **Downloads**.

Importar uma seleção de eventos

O Kaspersky Security Center Cloud Console permite importar uma seleção de eventos a partir do arquivo KLO. O arquivo KLO contém a seleção de eventos exportada e suas configurações.

Para importar uma seleção de eventos:

1. No menu principal, acesse **Monitoramento e relatórios → Seleções de eventos**.
2. Clique no botão **Importar** e escolha um arquivo de seleção de eventos que deseja importar.

3. Na janela aberta, especifique o caminho para o arquivo KLO e clique no botão **Abrir**. Observe que é possível selecionar apenas um arquivo de seleção de eventos.

   O processamento da seleção de eventos é iniciado.

A notificação com os resultados da importação é exibida. Caso a seleção de eventos seja importada com êxito, será possível clicar no link **Exibir detalhes da importação** para exibir as propriedades da seleção de eventos.

Após a importação ser concluída com êxito, a seleção de eventos será exibida na lista de seleção. As configurações da seleção de eventos também são importadas.

Caso a seleção de eventos recém-importada tenha um nome idêntico ao de seleção de eventos existente, o nome da seleção importada será expandido com o índice **(<próximo número da sequência>)**, por exemplo: **(1)**, **(2)**.

Visualização dos detalhes de um evento

Para visualizar detalhes de um evento:

1. Nova seleção de eventos.
2. Clique na hora do evento necessário.

   A janela **Propriedades do evento** se abre.
3. Na janela exibida, você pode fazer o seguinte:
   - Visualizar as informações sobre o evento selecionado
   - Ir ao evento anterior e ao seguir no resultado da seleção de eventos
   - Ir ao dispositivo no qual o evento ocorreu
   - Ir ao grupo de administração que inclui o dispositivo no qual o evento ocorreu
   - Para um evento relacionado a uma tarefa, vá às propriedades da tarefa

Exportar eventos para um arquivo

Para exportar eventos para um arquivo:

1. Nova seleção de eventos.
2. Selecione a caixa de seleção junto ao evento necessário.
3. Clique no botão **Exportar para arquivo**.

O evento selecionado é exportado para um arquivo.

Visualização de um histórico de eventos a partir de um evento

De um evento de criação ou modificação de um objeto que não tem suporte no gerenciamento de revisão, você pode alternar para o histórico de revisões do objeto.

Para visualizar o histórico de revisões de um evento:

1. Nova seleção de eventos.
2. Selecione a caixa de seleção junto ao evento necessário.
3. Clique no botão **Histórico de revisões**.

O histórico de revisões do objeto é aberto.

Registro de informações sobre eventos para tarefas e políticas

Esta seção oferece recomendações sobre como minimizar o número de eventos para as tarefas e políticas armazenadas no banco de dados do Kaspersky Security Center Cloud Console. Por padrão, cada 1.000 dispositivos têm 100.000 eventos. Caso o limite seja excedido, novos eventos substituem os antigos. Assim, eventos críticos podem desaparecer. Além disso, o evento de advertência do Servidor de Administração nomeado **O limite de eventos no banco de dados foi excedido. Os eventos foram excluídos** pode ocorrer. Nesses casos, recomendamos seguir as instruções nesta seção.

Assim, a velocidade de execução de cenários associados à análise dos eventos aumentará. Além disso, estas recomendações ajudam a reduzir o risco de que eventos críticos sejam substituídos por um grande número de eventos.

Por padrão, as propriedades de cada tarefa e política fornecem o armazenamento de todos os eventos relativos à execução da tarefa e da obrigatoriedade da política. No entanto, caso uma tarefa seja executada com frequência (por exemplo, mais de uma vez por semana), o número de eventos pode acabar sendo grande demais e os eventos podem inundar o banco de dados. Nesse caso, recomendamos selecionar uma das duas opções nas configurações da tarefa:

- **Salvar eventos relacionados ao progresso da tarefa**. Nesse caso, o Kaspersky Security Center Cloud Console armazena somente informações sobre a inicialização, andamento e conclusão da tarefa (com êxito, com um aviso ou erro) de cada dispositivo em que a tarefa for executada.
- **Salvar apenas os resultados da execução da tarefa**. Nesse caso, o Kaspersky Security Center Cloud Console armazena somente informações sobre a conclusão da tarefa (com êxito, com um aviso ou erro) de cada dispositivo em que a tarefa for executada.

Caso uma política tenha sido definida para um número bastante grande de dispositivos (por exemplo, mais de 10.000), o número de eventos também pode acabar sendo grande, e os eventos podem inundar o banco de dados. Nesse caso, recomendamos selecionar somente os eventos mais críticos nas configurações da política e ativar seu registro. Você é aconselhado a desativar o registro de todos outros eventos.

Você também pode reduzir o período de armazenamento para eventos associados com uma tarefa ou política. O período padrão é de 7 dias para eventos relacionados à tarefa e de 30 dias para eventos relacionados à política. Ao modificar o período de armazenamento do evento, considere os procedimentos de trabalho em vigor na sua organização e quanto tempo o administrador de sistema pode dedicar à análise de cada evento.

É aconselhável modificar as configurações de armazenamento de eventos caso os eventos sobre as alterações nos status intermediários de tarefas de grupo e os eventos sobre a aplicação de políticas ocuparem uma grande parte de todos os eventos no banco de dados do Kaspersky Security Center Cloud Console.

Excluir os eventos

Para excluir um ou vários eventos:

1. Nova seleção de eventos.
2. Selecione as caixas de seleção junto aos eventos necessários.
3. Clique no botão **Excluir**.

Os eventos selecionados são excluídos e não podem ser restaurados.

Excluir as seleções de eventos

Você pode excluir apenas as seleções de eventos definidas pelo usuário. As seleções de eventos predefinidas não podem ser excluídas.

Para excluir uma ou várias seleções de eventos:

1. No menu principal, acesse **Monitoramento e relatórios → Seleções de eventos**.
2. Marque as caixas de seleção ao lado das seleções de eventos que deseja excluir.
3. Clique em **Excluir**.
4. Na janela que se abre, clique em **OK**.

A seleção de eventos é excluída.

Notificações e status do dispositivo

Esta seção contém informações sobre como visualizar notificações, configurar a entrega de notificações, usar os status do dispositivo e habilitar a alteração de status do dispositivo.

Sobre notificações

O Kaspersky Security Center Cloud Console oferece a capacidade de controlar a rede da sua organização enviando notificações sobre qualquer evento que você considera importante. Para qualquer evento, você pode configurar as notificações por e-mail.

Para receber notificações por e-mail, você pode decidir a sua resposta para um evento. Essa resposta precisa ser a mais apropriada para a rede da sua organização.

Configurar a alternância dos status do dispositivo

Você pode alterar as condições para atribuir o status *Crítico* ou *Advertência* para um dispositivo.

Para ativar a alteração do status do dispositivo para Crítico:

1. No menu principal, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Crítico**.
5. No painel direito, na seção **Se especificados, definir como Crítico**, ative a condição para alterar o status de um dispositivo para *Crítico*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.

9. Clique em **OK**.

Quando condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Crítico*.

Para ativar a alteração do status do dispositivo para Advertência:

1. No menu principal, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Advertência**.
5. No painel direito, na seção **Se especificados, definir como Advertência**, ative a condição para alterar o status de um dispositivo para *Advertência*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.
9. Clique em **OK**.

Quando as condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Advertência*.

Configurar a entrega de notificações

Você pode configurar a notificação por e-mail sobre eventos que ocorrem no Kaspersky Security Center Cloud Console.

Para configurar a entrega de notificação de eventos que ocorrem no Kaspersky Security Center Cloud Console:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.
2. Clique na seção **Notificação** e, no painel direito, defina as configurações da notificação por e-mail:

   Destinatários (endereços de e-mail)

   Especifique os endereços de e-mail aos quais o Kaspersky Security Center Cloud Console enviará notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula.

   É possível especificar até 24 endereços de e-mail.
3. Clicar no botão **Enviar mensagem de teste** permite-lhe verificar se você configurou as notificações apropriadamente: o aplicativo envia uma notificação de teste aos endereços de e-mail que você especificou.
4. Clique no botão **OK** para fechar a janela de propriedades do Servidor de Administração.

As configurações de entrega de notificação salvas são aplicadas a todos os eventos que ocorrem no Kaspersky Security Center Cloud Console.

Você pode ignorar as configurações de entrega de notificações para certos eventos na seção **Configuração de eventos** das configurações do Servidor de Administração, de uma política ou de um aplicativo.

Novidades da Kaspersky

Esta seção descreve como usar, configurar e desativar o recebimento de Novidades da Kaspersky.

Sobre as Novidades Kaspersky

A seção Novidades Kaspersky (**Monitoramento e relatórios → Novidades Kaspersky**) apresenta as últimas novidades sobre a sua versão do Kaspersky Security Center Cloud Console e sobre aplicativos gerenciados instalados nos dispositivos gerenciados. O Kaspersky Security Center Cloud Console atualiza periodicamente as informações da seção, removendo informações antigas e adicionando novas.

O Kaspersky Security Center Cloud Console mostra apenas os comunicados Kaspersky relacionados ao Servidor de Administração conectado atualmente e aos aplicativos Kaspersky instalados nos dispositivos gerenciados deste Servidor de Administração. Os anúncios são mostrados individualmente para qualquer tipo de Servidor de Administração, seja principal, secundário ou virtual.

Se vários administradores usam o Kaspersky Security Center Cloud Console e definem diferentes idiomas de interface, o Kaspersky Security Center Cloud Console exibe os comunicados Kaspersky em todos os idiomas usados pelos administradores. Ao alterar o idioma da interface, os comunicados Kaspersky no idioma selecionado são adicionados à seção automaticamente, após você sair do console e entrar novamente.

Os informativos incluem informações dos seguintes tipos:

- Comunicados relacionados à segurança

  Os informativos relacionados à segurança têm como objetivo manter os aplicativos da Kaspersky instalados em sua rede atualizados e totalmente funcionais. Os informativos podem incluir informações sobre atualizações críticas para aplicativos da Kaspersky, correções para vulnerabilidades encontradas e maneiras de corrigir outros problemas em aplicativos da Kaspersky. Informativos relacionados à segurança são ativados por padrão. Se não deseja receber informações sobre novidades da Kaspersky, pode desativar este recurso.

  > Você não pode desativar as comunicações relacionadas à segurança no modo de avaliação do Kaspersky Security Center Cloud Console.

  Para mostrar a você as informações que correspondem à sua configuração de proteção de rede, o Kaspersky Security Center Cloud Console envia dados para os servidores em nuvem da Kaspersky e recebe apenas os informativos relacionados aos aplicativos Kaspersky instalados na rede. O conjunto de dados que pode ser enviado aos servidores é descrito no Contrato do Kaspersky Security Center Cloud Console. que você aceita ao criar um espaço de trabalho da empresa.

- Informativos de marketing

  Informativos de marketing incluem informações sobre ofertas especiais para os aplicativos da Kaspersky, anúncios e notícias da Kaspersky. Informativos de marketing estão desativados por padrão. Você recebe esse tipo de informativo apenas se ativou a Kaspersky Security Network (KSN). Você pode desativar os informativos de marketing desativando a KSN.

  Para que você visualize apenas informações relevantes que podem ser úteis na proteção de seus dispositivos de rede e em suas tarefas diárias, o Kaspersky Security Center Cloud Console envia dados para os servidores Kaspersky na nuvem e coleta os informativos apropriados. O conjunto de dados que pode ser enviado aos servidores é descrito na seção Dados Processados do Declaração da KSN.

As novas informações são divididas nas seguintes categorias, de acordo com a importância:

1. Informações críticas
2. Notícias importantes
3. Advertência

4. Informação

Quando as novas informações são exibidas na seção Novidades Kaspersky, o Kaspersky Security Center Cloud Console exibe um rótulo com uma notificação correspondente ao nível de importância da informação. Você pode clicar no rótulo para ver a notícia na seção Novidades Kaspersky.

Desativando o recebimento de Novidades Kaspersky

A seção Novidades Kaspersky (**Monitoramento e relatórios** → **Novidades Kaspersky**) apresenta as últimas novidades sobre a sua versão do Kaspersky Security Center Cloud Console e sobre aplicativos gerenciados instalados nos dispositivos gerenciados. Se não deseja receber informações de novidades sobre a Kaspersky, pode desativar este recurso.

Os informativos da Kaspersky incluem dois tipos de informações: informativos relacionados à segurança e de marketing. Você pode desativar os informativos de cada tipo separadamente.

> Você não pode desativar as comunicações relacionadas à segurança no modo de avaliação do Kaspersky Security Center Cloud Console.

Para desativar informativos relacionados à segurança:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.
   A janela Propriedades do Servidor de Administração é aberta.
2. Na guia **Geral**, selecione a seção **Novidades Kaspersky**.
3. Use o botão de alternância para mudar para a posição **Comunicados relacionados à segurança Desativado**.
4. Clique no botão **Salvar**.
   O recebimento de novidades sobre a Kaspersky está desativado.

Informativos de marketing estão desativados por padrão. Você recebe informativos de marketing apenas se ativou a Kaspersky Security Network (KSN). Você pode desativar este tipo de informativo desativando a KSN.

Para desativar os informativos de marketing:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.
   A janela Propriedades do Servidor de Administração é aberta.
2. Na guia **Geral**, selecione a seção **Configurações do KSN**.
3. Desative a opção **Concordo em usar a Kaspersky Security Network**.
4. Clique no botão **Salvar**.
   Os informativos de marketing estão desativados.

Receber aviso de expiração de licença

Para adicionar uma chave de licença do Kaspersky Endpoint Security for Business Select ao Servidor de Administração:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Chaves de licença**.

3. Clique em **Selecionar**.

4. Na janela que se abre, selecione sua licença e clique em **OK**.

   Como alternativa, se nenhuma licença for exibida, é possível clicar em **Adicionar nova chave de licença** e usar seu código de ativação.

A licença é adicionada ao Repositório do servidor de administração. Isso faz com que o Servidor de Administração gere um evento crítico *A licença expira em breve* um dia antes do término do prazo da licença e um evento crítico de *Modo de funcionalidade limitada* após o término do período da licença. Se desejar, é possível configurar a entrega da notificação.

Ao adicionar uma chave de licença do Kaspersky Endpoint Security for Business Select ao Repositório do servidor de administração, a licença será considerada usada em um dispositivo.

Cloud Discovery

O Kaspersky Security Center Cloud Console permite monitorar o uso de serviços em nuvem em dispositivos gerenciados que executam o Windows e bloquear o acesso a serviços em nuvem que considerar indesejados. A Cloud Discovery rastreia as tentativas do usuário de obter acesso a esses serviços por meio de navegadores e aplicativos desktop. Ele também rastreia as tentativas do usuário de obter acesso aos serviços em nuvem por meio de conexões não criptografadas (por exemplo, usando o protocolo HTTP). Esse recurso ajuda você a detectar e interromper o uso de serviços em nuvem por meio de shadow IT.

O recurso Cloud Discovery só estará disponível se você tiver adquirido uma das licenças do Kaspersky NEXT. Para detalhes, consulte Licenças e quantidade mínima de dispositivos para cada licença.

O recurso de bloqueio está disponível somente se você usar o Kaspersky Endpoint Security 11.2 for Windows ou posterior. As versões anteriores do aplicativo de segurança só permitem monitorar o uso de serviços em nuvem.

Você pode ativar o recurso Cloud Discovery e selecionar as políticas ou perfis de segurança para os quais deseja ativar o recurso. Você também pode ativar ou desativar o recurso separadamente em cada política ou perfil de segurança. Você pode bloquear o acesso a serviços em nuvem que outros usuários não devem acessar.

O widget do Cloud Discovery e os relatórios do Cloud Discovery exibem informações sobre tentativas bem-sucedidas e bloqueadas de obtenção de acesso aos serviços em nuvem. O widget também exibe o nível de risco de cada serviço em nuvem. O Kaspersky Security Center Cloud Console obtém informações sobre o uso de serviços em nuvem de todos os dispositivos gerenciados protegidos somente pelas políticas ou perfis de segurança e que tenham o recurso ativado.

Como ativar e desativar o Cloud Discovery

O recurso Cloud Discovery permite a você obter informações sobre o uso de serviços em nuvem de todos os dispositivos gerenciados protegidos somente pelas políticas de segurança e que tenham o recurso ativado. Observe que você pode ativar ou desativar o Cloud Discovery somente para a política do Kaspersky Endpoint Security for Windows.

Para poder ativar e desativar o Cloud Discovery, você deve ter direitos de **Gravar** na área funcional **Recursos gerais: Funcionalidade básica**.

Você pode ativar ou desativar o recurso Cloud Discovery nos parâmetros da política do Kaspersky Endpoint Security for Windows e usando o widget depois de adicioná-lo ao painel.

Para ativar ou desativar o recurso Cloud Discovery nas propriedades da política do Kaspersky Endpoint Security for Windows:

1. Acesse o Kaspersky Security Center Cloud Console.
2. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
3. Clique no nome da Política do Kaspersky Endpoint Security for Windows.

   A janela Propriedades da política do Kaspersky Endpoint Security for Windows será aberta.
4. Vá para a seção **Configurações do aplicativo** → **Controles de segurança** → **Cloud Discovery**.
5. Na janela do **Cloud Discovery** que se abre, execute uma das seguintes ações:

   - Para ativar o recurso, ative a opção **Cloud Discovery DESATIVADO**.

     Na **tabela Nome do serviço e nível de risco** exibida, você pode bloquear o acesso a um serviço específico ou a toda a categoria de uma só vez.

     O widget do **Cloud Discovery** exibirá informações no painel.

   - Para desativar o recurso, desative a opção **Cloud Discovery ATIVADO**.

     O widget do **Cloud Discovery** não exibirá informações no painel.

O Cloud Discovery estará ativado ou desativado na política de segurança selecionada.

Como adicionar o widget Cloud Discovery ao painel

Você pode adicionar o widget do **Cloud Discovery** ao painel para monitorar o uso de serviços em nuvem em dispositivos gerenciados.

Para poder adicionar o widget do Cloud Discovery ao painel, você deve ter direitos de **Gravar** na área funcional **Recursos gerais: Funcionalidade básica**.

Para adicionar o widget do Cloud Discovery ao painel:

1. Acesse o Kaspersky Security Center Cloud Console.

2. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.

3. Clique no botão **Adicionar ou restaurar widget da Web**.

4. Na lista de widgets disponíveis, clique no ícone de divisa (›) ao lado da categoria **Outro**.

5. Selecione o widget do **Cloud Discovery** e clique no botão **Adicionar**.

   O widget selecionado é adicionado no final do painel.

6. Se o recurso **Cloud Discovery** estiver desativado nas propriedades da política do Kaspersky Endpoint Security for Windows, faça o seguinte:

   a. No widget do **Cloud Discovery**, clique no botão **Ativar**.

   b. Na janela **Ativar o Cloud Discovery** exibida, selecione as políticas de segurança para as quais você deseja ativar o recurso e clique no botão **Ativar**.

      Observe que as seguintes configurações de política serão ativadas automaticamente: **Injetar script no tráfego da Web para interagir com páginas da Web**, **Monitor de sessão da Web** e **Verificação de conexões criptografadas**.

O **Cloud Discovery** estará ativado para as políticas de segurança selecionadas e o widget estará adicionado ao painel.

Exibir informações sobre o uso de serviços em nuvem

Você pode exibir o widget do **Cloud Discovery**, que exibe informações sobre tentativas de obtenção de acesso aos serviços em nuvem. O widget também exibe o nível de risco de cada serviço em nuvem. O Kaspersky Security Center Cloud Console obtém informações sobre o uso de serviços em nuvem de todos os dispositivos gerenciados protegidos somente pelas políticas de segurança e que tenham o recurso ativado.

Antes de visualizar, certifique-se de que:

- o recurso Cloud Discovery esteja ativado na política do Kaspersky Endpoint Security for Windows.
- o widget do **Cloud Discovery** esteja adicionado ao painel.
- você tenha os direitos de **Ler** na área funcional **Recursos gerais: Funcionalidade básica**.

Para visualizar o widget do Cloud Discovery:

1. Acesse o Kaspersky Security Center Cloud Console.

2. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.

   O widget do **Cloud Discovery** será exibido no painel.

3. No lado esquerdo do widget do **Cloud Discovery**, selecione uma categoria de serviços em nuvem.

   A tabela no lado direito do widget exibe até cinco serviços, da categoria selecionada, aos quais os usuários tentam obter acesso com mais frequência. As tentativas bem-sucedidas e bloqueadas são contabilizadas.

4. No lado direito do widget, selecione um serviço específico.

   A tabela abaixo exibe até dez dispositivos que tentam obter acesso ao serviço com mais frequência.

O widget exibe as informações solicitadas.

No widget exibido, você pode fazer o seguinte:

- Prossiga para a seção **Monitoramento e relatórios** → **Relatórios** para visualizar os relatórios do Cloud Discovery.
- Bloquear ou permitir acesso ao serviço de nuvem selecionado.

O recurso de bloqueio está disponível somente se você tiver adquirido uma das licenças do Kaspersky Next. Para detalhes, consulte Licenças e quantidade mínima de dispositivos para cada licença.

Nível de risco de um serviço de nuvem

Para cada serviço em nuvem, o Cloud Discovery fornece um nível de risco. O nível de risco ajuda a determinar os serviços que não atendem aos requisitos de segurança de sua organização. Por exemplo, é possível levar em consideração o nível de risco ao decidir se deve bloquear o acesso a um determinado serviço.

Isenção de responsabilidade: o nível de risco é um índice estimado e não diz nada sobre a qualidade de um serviço em nuvem ou sobre o fabricante do serviço. O nível de risco é simplesmente uma recomendação dos especialistas da Kaspersky.

Os níveis de risco dos serviços em nuvem são exibidos no widget do Cloud Discovery e na lista de todos os serviços em nuvem monitorados.

Como bloquear o acesso a serviços de nuvem indesejados

Você pode bloquear o acesso a serviços em nuvem que outros usuários não devem acessar. Você também pode permitir o acesso a serviços em nuvem que foram bloqueados anteriormente.

Entre outras considerações, é possível levar em consideração o nível de risco ao decidir se deve bloquear o acesso a um determinado serviço.

Você pode bloquear ou permitir o acesso aos serviços em nuvem para determinada política ou perfil de segurança.

Para bloquear ou permitir o acesso a um serviço em nuvem:

1. Abra o widget do Cloud Discovery e selecione o serviço em nuvem desejado.
2. No painel **Dez dispositivos que mais usam o painel de serviço**, localize a política ou o perfil de segurança para o qual você deseja bloquear ou permitir o serviço.
3. Na linha desejada, na coluna **Status de acesso na política ou nos perfis**, execute uma das seguintes ações:
   - Para bloquear o serviço, selecione **Bloqueado** na lista suspensa.
   - Para permitir o serviço, selecione **Permitido** na lista suspensa.
4. Clique no botão **Salvar**.

O acesso ao serviço selecionado estará bloqueado ou permitido para a política ou o perfil de segurança.

Diagnóstico remoto de dispositivos cliente

É possível usar o diagnóstico remoto para execução remota das seguintes operações nos dispositivos clientes baseados em Windows e Linux:

- Ativar e desativar o rastreamento, alterar o nível de rastreamento e baixar o arquivo de rastreamento
- Download de informações do sistema e de configurações do aplicativo
- Download de registros de eventos
- Gerar um arquivo de dump para um aplicativo
- Início do diagnóstico e download de seus relatórios
- Início, interrupção e reinício de aplicativos

Você pode usar registros de eventos e relatórios de diagnóstico baixados de um dispositivo cliente para resolver problemas. Além disso, ao entrar em contato com o Suporte Técnico da Kaspersky, um especialista de Suporte Técnico pode pedir que você faça download de arquivos de rastreamento, arquivos de despejo, logs de eventos e relatórios de diagnóstico de um dispositivo cliente para análise adicional na Kaspersky.

Abertura da janela de diagnóstico remoto

Para executar diagnóstico remoto em dispositivos clientes baseados em Windows e Linux, é necessário abrir a janela de diagnóstico remoto.

Para abrir a janela de diagnóstico remoto:

1. Para selecionar o dispositivo para o qual você deseja abrir a janela de diagnóstico remoto, execute um dos seguintes procedimentos:
   - Se o dispositivo pertencer a um grupo de administração, vá para **Ativos (dispositivos)** → **Grupos** → **<nome do grupo>** → **Dispositivos gerenciados**.
   - Caso o dispositivo pertença ao grupo de dispositivos não atribuídos, No menu principal, vá para **Descoberta e implementação** → **Dispositivos não atribuídos**.
2. Clique no nome do dispositivo necessário.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Avançado**.
4. Na janela que é aberta, clique em **Diagnóstico remoto**.

   Isso abre a janela de **Diagnóstico remoto** do dispositivo cliente. Caso a conexão entre o Servidor de Administração e o dispositivo cliente não seja estabelecida, uma mensagem de erro é exibida.

Como alternativa, caso precise obter todas as informações de diagnóstico sobre um dispositivo cliente baseado em Linux de uma só vez, é possível executar o script collect.sh nesse dispositivo.

Ativação e desativação do rastreamento para aplicativos

É possível ativar e desativar o rastreamento para aplicativos, incluindo o rastreamento do Xperf.

Ativação e desativação do rastreamento

Para ativar ou desativar o rastreamento em um dispositivo remoto:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione o aplicativo para o qual deseja ativar ou desativar o rastreamento.

   A lista de opções de diagnóstico remoto é aberta.
4. Se desejar ativar o rastreamento:

   a. Na seção **Rastreamento**, clique em **Ativar rastreamento**.

   b. Na janela **Modificar nível de rastreamento** que se abre, recomendamos que você mantenha os valores padrões das configurações. Quando necessário, um especialista de Suporte Técnico orientará você através do processo de configuração. Estão disponíveis as seguintes configurações:

   - **Nível de rastreamento**

     O nível de rastreamento define o volume de detalhes que o arquivo de rastreamento contém.

   - **Rastreamento baseado em rotatividade**

     O aplicativo sobrescreve as informações de rastreamento para impedir o aumento excessivo no tamanho do arquivo de rastreamento. Especifique o número máximo de arquivos a serem usados para armazenar as informações de rastreamento e o tamanho máximo de cada arquivo. Se o número máximo de arquivos de rastreamento com o tamanho máximo estiver gravado, o arquivo de rastreamento mais antigo será excluído para que um novo arquivo possa ser gravado.

     Essa configuração está disponível apenas para o Kaspersky Endpoint Security.

   c. Clique em **Salvar**.

   O rastreamento está ativado para o aplicativo selecionado. Em alguns casos, um aplicativo de segurança e sua tarefa devem ser reiniciados para que seja possível ativar o rastreamento.

   Em dispositivos clientes baseados em Linux, o rastreamento do componente Atualizador do Kaspersky Security Agent é regulado pelas configurações do Agente de Rede. Portanto, as opções **Ativar rastreamento** e **Modificar nível de rastreamento** estão desativadas para este componente em dispositivos clientes que executam o Linux.
5. Caso deseje desativar o rastreamento para o aplicativo selecionado, clique em **Desabilitar rastreamento**.

   O rastreamento está desativado para o aplicativo selecionado.

Ativação do rastreamento do Xperf

Para o Kaspersky Endpoint Security, um especialista de Suporte Técnico pode solicitar que você ative o rastreamento do Xperf para obter informações sobre o desempenho do sistema.

Para ativar e configurar o rastreamento do Xperf ou desativá-lo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione Kaspersky Endpoint Security for Windows.

   A lista de opções de diagnóstico remoto do Kaspersky Endpoint Security for Windows é exibida.
4. Na seção **Rastreamento do Xpref** da lista, clique em **Ativar rastreamento Xperf**.

   Se o rastreamento do Xperf já estiver ativado, o botão **Desativar rastreamento Xperf** é exibido. Clique neste botão caso queira desativar o rastreamento do Xperf para o Kaspersky Endpoint Security for Windows.
5. Na janela **Alterar nível de rastreamento Xperf** que se abre, dependendo da solicitação do especialista de Suporte Técnico, faça o seguinte:

   a. Selecione um dos seguintes níveis de rastreamento:

   - **Nível leve**

     Um arquivo de rastreamento deste tipo contém a quantidade mínima de informações sobre o sistema.

     Por padrão, esta opção está selecionada.

   - **Nível profundo**

     Um arquivo de rastreamento deste tipo contém informações mais detalhadas do que as dos arquivos de rastreamento do tipo *Superficial* e podem ser solicitadas pelos especialistas de Suporte Técnico quando um arquivo de rastreamento do tipo *Superficial* não for suficiente para a avaliação de desempenho. Um arquivo de rastreamento *Profundo* contém informações técnicas sobre o sistema, como as informações sobre hardware, sistema operacional, lista de processos e aplicativos iniciados e concluídos, eventos usados para avaliação de desempenho e eventos da Ferramenta de Avaliação de Sistema do Windows.

   b. Selecione um dos seguintes tipos de rastreamento do Xperf:

   - **Tipo básico**

     As informações de rastreamento são recebidas durante a operação do aplicativo Kaspersky Endpoint Security.

     Por padrão, esta opção está selecionada.

   - **Tipo na reinicialização**

As informações de rastreamento são recebidas quando o sistema operacional é iniciado no dispositivo gerenciado. Esse tipo de rastreamento é eficaz quando o problema que afeta o desempenho do sistema ocorre depois que o dispositivo é ligado e antes da inicialização do Kaspersky Endpoint Security.

Você também pode receber a solicitação de ativar a opção **Tamanho do arquivo de rotatividade, em MB** para impedir o aumento excessivo no tamanho do arquivo de rastreamento. Especifique o tamanho máximo do arquivo de rastreamento. Quando o arquivo atingir o tamanho máximo, as informações de rastreamento mais antigas serão substituídas por novas informações.

c. Defina o tamanho do arquivo de rotação.

d. Clique em **Salvar**.

O rastreamento do Xperf está ativado e configurado.

6. Caso queira desativar o rastreamento do Xperf para o Kaspersky Endpoint Security for Windows, clique em **Desativar rastreamento Xperf** na seção **Rastreamento do Xpref**.

   O rastreamento do Xperf está desativado.

Download de arquivos de rastreamento de um aplicativo

É possível baixar os arquivos de rastreamento a partir de um dispositivo cliente se apenas uma das duas condições a seguir for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo, um servidor push estive em uso ou um gateway de conexão estiver em uso. Caso contrário, não será possível fazer o download.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Para fazer download do arquivo de rastreamento de um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.

2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.

3. Na lista de aplicativos, selecione o aplicativo para o qual deseja baixar o arquivo de rastreamento.

4. Na seção **Rastreamento**, clique no botão **Arquivos de rastreamento**.

   Assim, a janela **Registros de rastreamento do dispositivo** é aberta, onde uma lista de arquivos de rastreamento é exibida.

5. Na lista de arquivos de rastreamento, selecione o arquivo que deseja baixar.

6. Execute uma das seguintes ações:

   - Faça o download do arquivo selecionado clicando em **Baixar**. É possível selecionar um ou vários arquivos para baixar.

   - Baixe uma parte do arquivo selecionado:

a. Clique em **Baixar uma parte**.

Não é possível baixar partes de vários arquivos ao mesmo tempo. Caso selecione mais de um arquivo de rastreamento, o botão **Baixar uma parte** será desativado.

b. Na janela exibida, especifique o nome e a parte do arquivo a ser baixada, de acordo com suas necessidades.

Para dispositivos baseados em Linux, a edição do nome da parte do arquivo não está disponível.

c. Clique em **Baixar**.

O arquivo selecionado, ou sua parte, é baixado no local especificado.

Exclusão de arquivos de rastreamento

É possível excluir arquivos de rastreamento que não sejam mais necessários.

Para excluir um arquivo de rastreamento:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto que é aberta, selecione a guia **Registros de evento**.
3. Na seção **Arquivos de rastreamento**, clique em **Logs do Windows Update** ou **Logs de instalação remota**, dependendo de quais arquivos de rastreamento deseja excluir.

   Assim, a janela **Registros de rastreamento do dispositivo** é aberta, onde uma lista de arquivos de rastreamento é exibida.
4. Na lista de arquivos de rastreamento, selecione um ou vários arquivos que deseja excluir.
5. Clique no botão **Remover**.

Os arquivos de rastreamento selecionados são excluídos.

Download das configurações do aplicativo

É possível baixar as configurações do aplicativo de um dispositivo cliente se apenas uma das condições a seguir for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo, um servidor push estiver em uso ou se um gateway de conexão estiver em uso. Caso contrário, não será possível fazer o download.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Para baixar as configurações do aplicativo a partir de um dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.
3. Na seção **Configurações do aplicativo**, clique no botão **Baixar** para baixar as informações sobre as configurações dos aplicativos instalados no dispositivo cliente.

O arquivo ZIP com as informações é baixado no local especificado.

Download das informações do sistema de um dispositivo cliente

É possível baixar as informações do sistema para o dispositivo a partir de um dispositivo cliente se apenas uma das seguintes condições for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo, um servidor push estiver em uso ou um gateway de conexão estiver em uso. Caso contrário, não será possível fazer o download.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Para baixar as informações do sistema a partir de um dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Informações do sistema**.
3. Clique no botão **Baixar** para baixar as informações do sistema sobre o dispositivo cliente.

O arquivo com as informações é baixado para o local especificado.

Download de registros de eventos

É possível baixar os logs de eventos para o seu dispositivo a partir de um dispositivo cliente se apenas uma das seguintes condições for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo, um servidor push estiver em uso ou um gateway de conexão estiver em uso. Caso contrário, não será possível fazer o download.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Para baixar um log de eventos a partir de um dispositivo remoto:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, na guia **Registros de evento**, clique em **Todos os logs do dispositivo**.
3. Na janela **Todos os logs do dispositivo**, selecione os logs relevantes.
4. Execute uma das seguintes ações:
   - Baixe o log selecionado clicando em **Baixar todo o arquivo**.
   - Baixe uma parte do log selecionado:
     a. Clique em **Baixar uma parte**.
     Não é possível baixar partes de vários logs ao mesmo tempo. Caso mais de uma política seja selecionada, o botão **Baixar uma parte** será desabilitado.
     b. Na janela exibida, especifique o nome e a parte do arquivo a ser baixada de acordo com suas necessidades.

c. Clique em **Baixar**.

O log de eventos selecionado, ou uma parte dele, é baixado no local especificado.

Início, interrupção e reinício do aplicativo

É possível iniciar, parar e reiniciar aplicativos em um dispositivo cliente.

Para iniciar, interromper ou reiniciar um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione o aplicativo que deseja iniciar, parar ou reiniciar.
4. Selecione uma ação clicando em um dos seguintes botões:

   - **Parar aplicativo**

     Esse botão está disponível apenas se o aplicativo estiver em execução no momento.
   - **Reiniciar aplicativo**

     Esse botão está disponível apenas se o aplicativo estiver em execução no momento.
   - **Iniciar aplicativo**

     Esse botão está disponível apenas se o aplicativo não estiver em execução no momento.

Dependendo da ação selecionada, o aplicativo necessário é iniciado, parado ou reiniciado no dispositivo cliente.

Se o Agente de Rede for reiniciado, será exibida uma mensagem informando que a conexão atual do dispositivo com o Servidor de Administração será perdida.

Execução do diagnóstico remoto de um aplicativo e download dos resultados

Para iniciar o diagnóstico para um aplicativo em um dispositivo remoto e baixar os resultados:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione o aplicativo para o qual deseja executar o diagnóstico remoto.

   A lista de opções de diagnóstico remoto é aberta.
4. Na seção **Relatório de diagnóstico**, clique no botão **Executar diagnósticos**.

   Isso inicia o processo de diagnóstico remoto e gera um relatório de diagnóstico. Quando o processo de diagnóstico estiver concluído, o botão **Baixar o relatório de diagnóstico** ficará disponível.

5. Clique no botão **Baixar o relatório de diagnóstico** para baixar o relatório.

O relatório é baixado no local especificado.

Execução de um aplicativo em um dispositivo cliente

Você pode ter que executar um aplicativo no dispositivo cliente se um especialista de suporte da Kaspersky solicitar. Não será necessário instalar o aplicativo no dispositivo. Não será necessário instalar o aplicativo no dispositivo.

Para executar um aplicativo no dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Executando um aplicativo remoto**.
3. Na seção **Arquivos do aplicativo**, clique no botão **Procurar** para selecionar um arquivo ZIP contendo o aplicativo que deseja executar no dispositivo cliente.

   O arquivo comprimido deve incluir a pasta do utilitário. Essa pasta contém o arquivo executável a ser executado em um dispositivo remoto.

   É possível especificar o nome do arquivo executável e os argumentos da linha de comando, caso seja necessário. Para fazer isso, preencha os campos **Arquivo executável em um arquivo comprimido para ser executado em um dispositivo remoto** e os campos **Argumentos da linha de comando**.
4. Clique no botão **Carregar e executar** para executar o aplicativo especificado em um dispositivo cliente.
5. Siga as instruções do especialista de suporte da Kaspersky.

Gerar um arquivo de dump para um aplicativo

Um arquivo de despejo do aplicativo permite visualizar os parâmetros do aplicativo em execução em um dispositivo cliente em um dado momento. Esse arquivo também contém informações sobre os módulos que foram carregados para um aplicativo.

A geração de arquivos de despejo está disponível apenas para processos de 32 bits em execução em dispositivos cliente baseados no Windows. Para dispositivos cliente que executam Linux e para processos de 64 bits, esse recurso não é compatível.

Para criar um arquivo de despejo para um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, clique na guia **Executando um aplicativo remoto**.
3. Na seção **Gerando o arquivo de dump do processo**, especifique o arquivo executável do aplicativo para o qual deseja gerar um arquivo de despejo.

4. Clique no botão **Baixar** para salvar o arquivo de despejo do aplicativo especificado.

   Caso o aplicativo especificado não esteja em execução no dispositivo cliente, a mensagem de erro será exibida.

Execução do diagnóstico remoto em um dispositivo cliente baseado em Linux

O Kaspersky Security Center Cloud Console permite baixar as informações básicas de diagnóstico de um dispositivo cliente. Como alternativa, é possível obter as informações de diagnóstico sobre um dispositivo baseado em Linux com o uso do script collect.sh da Kaspersky. Esse script é executado no dispositivo cliente baseado em Linux que precisa ser diagnosticado. Em seguida, ele gera um arquivo com as informações de diagnóstico, as informações do sistema sobre esse dispositivo, os arquivos de rastreamento de aplicativos, os logs do dispositivo e um arquivo de despejo para os arquivos encerrados por emergência.

Recomendamos usar o script collect.sh para obter todas as informações de diagnóstico sobre o dispositivo cliente baseado em Linux de uma só vez. Se você baixar as informações de diagnóstico remotamente por meio do Kaspersky Security Center Cloud Console, precisará passar por todas as seções da interface de diagnóstico remoto. Além disso, as informações de diagnóstico para um dispositivo baseado em Linux provavelmente não serão obtidas completamente.

Se você precisar enviar o arquivo gerado com as informações de diagnóstico ao Suporte técnico da Kaspersky, exclua todas as informações confidenciais antes de enviar o arquivo.

Para baixar as informações de diagnóstico de um dispositivo cliente baseado em Linux usando o script collect.sh:

1. Baixe o script collect.sh compactado no arquivo collect.tar.gz.
2. Copie o arquivo baixado para o dispositivo cliente baseado em Linux que precisa ser diagnosticado.
3. Execute o seguinte comando para descompactar o arquivo collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Execute o seguinte o comando para especificar os direitos de execução do script:

   ```
   # chmod +x collect.sh
   ```

5. Execute o script collect.sh usando uma conta com direitos de administrador:

   ```
   # ./collect.sh
   ```

Um arquivo com as informações de diagnóstico é gerado e salvo na pasta /tmp/$HOST_NAME-collect.tar.gz.

Exportando eventos para os sistemas SIEM

Esta seção descreve como configurar a exportação de eventos para os sistemas SIEM.

Cenário: configurando a exportação de eventos para um sistema SIEM

Esta seção apresenta um cenário para configurar a exportação de eventos do Servidor de Administração para sistemas SIEM externos. Exportar informações sobre eventos para sistemas SIEM externos permite aos administradores de sistemas SIEM responderem prontamente aos eventos de sistema de segurança que ocorrem em dispositivos gerenciados ou em grupos de dispositivos.

Pré-requisitos

Antes de começar a configurar a exportação de eventos no Kaspersky Security Center Cloud Console:

- Saiba mais sobre os métodos de exportação de eventos.
- Certifique-se de conhecer os valores das configurações do sistema.

Você pode executar as etapas deste cenário em qualquer ordem.

Fases

O processo de exportação de eventos para o sistema SIEM consiste nas seguintes etapas:

- **Configurando o sistema SIEM para receber eventos do Kaspersky Security Center Cloud Console**

  Você deve configurar o recebimento de eventos do Kaspersky Security Center Cloud Console no sistema SIEM.

- **Marcando eventos para exportação**

  Você deve marcar quais eventos deseja exportar para o sistema SIEM. Em primeiro lugar, marque os eventos gerais que ocorrem em todos os aplicativos gerenciados da Kaspersky. Além disso, é possível marcar os eventos para aplicativos gerenciados da Kaspersky específicos.

- **Configurando o Kaspersky Security Center Cloud Console para exportação de eventos para o sistema SIEM**

  Você deve configurar o Kaspersky Security Center Cloud Console para iniciar a exportação de eventos para o sistema SIEM.

Resultados

Após configurar a exportação de eventos para o sistema SIEM, você pode ver os resultados de exportação se tiver selecionado eventos que deseja exportar.

Antes de iniciar

Ao configurar uma exportação automática de eventos no Kaspersky Security Center Cloud Console, você deve especificar algumas das configurações do sistema SIEM. Recomenda-se que você verifique estas configurações com antecedência para preparar-se para configurar o Kaspersky Security Center Cloud Console.

Para configurar com êxito o envio automático de eventos a um sistema SIEM, você deve conhecer as seguintes configurações:

- **Endereço do servidor do sistema SIEM**

  O endereço IP do servidor onde o sistema SIEM atualmente usado está instalado. Verifique este valor nas suas configurações de sistema SIEM.

- **Porta do servidor do sistema SIEM**

  O número da porta usada para estabelecer a conexão entre o Kaspersky Security Center Cloud Console e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center Cloud Console e nas configurações do receptor do seu sistema SIEM.

- **Protocolo**

  Protocolo usado para transferir mensagens do Kaspersky Security Center Cloud Console ao seu sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center Cloud Console e nas configurações do receptor do seu sistema SIEM.

Sobre a exportação de evento

O Kaspersky Security Center Cloud Console permite receber informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nos dispositivos gerenciados. As informações sobre eventos são salvas no banco de dados do Servidor de Administração.

Você pode usar a exportação de evento dentro de sistemas centralizados que tratam de questões de segurança em nível organizacional e técnico, que fornecem serviços de monitoramento da segurança e consolidam informações de diferentes soluções. Estes são sistemas SIEM, que fornecem a análise em tempo real de alertas de segurança e eventos gerados por hardware de rede e aplicativos ou Centros de Operação de Segurança (SOCs).

Estes sistemas recebem dados de muitas fontes, incluindo redes, segurança, servidores, bancos de dados e aplicativos. Os sistemas de SIEM também fornecem a funcionalidade para consolidar os dados monitorados para ajudá-lo a evitar faltar a eventos críticos. Além disso, os sistemas executam a análise automatizada de eventos correlacionados e alertas para notificar os administradores de problemas de segurança imediatos. Um alerta pode ser implementado através de um painel ou pode ser enviado por canais de terceiros, tal como por um e-mail.

O processo de exportar eventos do Kaspersky Security Center Cloud Console para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center Cloud Console) e um receptor do evento (sistema SIEM). Para exportar com sucesso eventos, você deve configurar isso no seu sistema SIEM e no Kaspersky Security Center Cloud Console. Não importa que lado você configura primeiro. Você pode configurar a transmissão de eventos no Kaspersky Security Center Cloud Console e depois configurar o recebimento de eventos pelo sistema SIEM, ou vice-versa.

Formato Syslog de exportação de eventos

Você pode enviar eventos no formato Syslog para qualquer sistema SIEM. Usando o formato Syslog, você pode encaminhar qualquer evento que ocorre no Servidor de Administração do e em aplicativos Kaspersky que são instalados em dispositivos gerenciados. Ao exportar eventos no formato Syslog, você pode selecionar exatamente quais tipos de eventos serão encaminhados ao sistema SIEM.

Recebimento de eventos pelo sistema SIEM

O sistema SIEM deve receber e corretamente analisar os eventos recebidos do Kaspersky Security Center Cloud Console. Para estes propósitos, você deve configurar apropriadamente o sistema SIEM. A configuração depende do sistema SIEM específico utilizado. No entanto, há um número de etapas gerais na configuração de todos os sistemas SIEM, tal como a configuração do receptor e do analisador.

Configurando a exportação de eventos em um sistema SIEM

O processo de exportar eventos do Kaspersky Security Center Cloud Console para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center Cloud Console) e um receptor do evento (sistema SIEM). Você deve configurar a exportação de eventos no seu sistema SIEM e no Kaspersky Security Center Cloud Console.

As configurações especificadas no sistema SIEM dependem de qual sistema que você estiver usando. Normalmente, para todos os sistemas SIEM você deve definir um receptor e, opcionalmente, um analisador de mensagem para analisar os eventos recebidos.

Configurar o receptor

Para poder receber eventos enviados pelo Kaspersky Security Center Cloud Console, configure o receptor no seu sistema SIEM. Em geral, as seguintes configurações devem ser especificadas no sistema SIEM:

- **Porta**

  Especifique o número da porta para se conectar ao Kaspersky Security Center Cloud Console. Esta porta deve ser a mesma especificada no Kaspersky Security Center Cloud Console durante a configuração com um sistema SIEM.

- **Protocolo de mensagem ou tipo de origem**

  Especifique o formato Syslog.

Dependendo do sistema SIEM usado, você deverá ter que especificar algumas configurações adicionais de receptor.

Analisadores de mensagem

Os eventos exportados são passados aos sistemas SIEM como mensagens. Estas mensagens devem ser apropriadamente analisadas para que as informações nos eventos possam ser usadas pelo sistema SIEM. Os analisadores de mensagem são uma parte do sistema SIEM e são usados para dividir o conteúdo da mensagem em campos relevantes, tal como ID do evento, gravidade, descrição, parâmetros e assim por diante. Isto ativa o sistema SIEM para processar eventos recebidos do Kaspersky Security Center Cloud Console para que eles possam ser armazenados no banco de dados do sistema SIEM.

Marcando eventos para exportação para sistemas SIEM em formato Syslog

Esta seção descreve como marcar eventos para exportação adicional para sistemas SIEM no formato Syslog.

Sobre a marcação de eventos para exportação para o sistema SIEM no formato Syslog

Após ativar a exportação automática de eventos, você deve marcar quais eventos serão exportados ao sistema SIEM externo.

Você pode configurar a exportação de eventos em formato Syslog para um sistema externo com base em uma das seguintes condições:

- Marcando eventos gerais. Se você marcar eventos para exportar em uma política, nas configurações de um evento ou no Servidor de Administração, o sistema SIEM receberá os eventos marcados que ocorreram em todos os aplicativos gerenciados pela política específica. Se os eventos exportados foram selecionados na política, você não será capaz de redefini-los para um aplicativo individual gerenciado por esta política.
- Marcando eventos para um aplicativo individual. Se você marcar eventos para exportar para um aplicativo gerenciado instalado em um dispositivo gerenciado, o sistema SIEM somente receberá os eventos que ocorreram neste aplicativo.

Marcando eventos de um aplicativo da Kaspersky para exportação em formato Syslog

Se você desejar exportar eventos que ocorreram em um aplicativo gerenciado específico instalado nos dispositivos gerenciados, marque os eventos para exportação na política do aplicativo. Nesse caso, os eventos marcados são exportados de todos os dispositivos incluídos no escopo da política.

Para marcar eventos para exportação para um aplicativo gerenciado específico:

1. No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique na política do aplicativo para o qual você deseja marcar eventos.

   A janela Propriedades da política será aberta.
3. Siga para a seção **Configuração de eventos**.
4. Marque as caixas de seleção ao lado dos eventos que você deseja exportar para um sistema SIEM.
5. Clique no botão **Marcar exportação para o sistema SIEM usando o Syslog**.

   Também é possível marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, que é aberta ao clicar no link do evento.
6. O sinal de verificação (✓) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.
7. Clique no botão **Salvar**.

Os eventos marcados do aplicativo gerenciado estão prontos para serem exportados para um sistema SIEM.

É possível marcar quais eventos exportar para um sistema SIEM para um dispositivo gerenciado específico. Se os eventos exportados anteriormente foram marcados em uma política de aplicativo, não será possível redefinir os eventos marcados para um dispositivo gerenciado.

Para marcar eventos para exportação para um dispositivo gerenciado:

1. No menu principal, vá para **Ativos (dispositivos)** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Clique no link com o nome do dispositivo desejado na lista de dispositivos gerenciados.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Siga para a seção **Aplicativos**.

4. Clique no link com o nome do aplicativo desejado na lista de aplicativos.

5. Siga para a seção **Configuração de eventos**.

6. Marque as caixas de seleção ao lado dos eventos que deseja exportar para um arquivo.

7. Clique no botão **Marcar exportação para o sistema SIEM usando o Syslog**.

   Além disso, você pode marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, aberta ao se clicar no link do evento.

8. O sinal de verificação (✓) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.

A partir de agora, o Servidor de Administração envia os eventos marcados para o sistema SIEM se a exportação para o sistema SIEM estiver configurada.

Marcando eventos gerais para exportação no formato Syslog

Você pode marcar eventos gerais que o Servidor de Administração exportará para os sistemas SIEM usando o formato Syslog.

Para configurar eventos gerais para um sistema SIEM:

1. Execute uma das seguintes ações:

   - No menu principal, clique no ícone de configurações (⚙) ao lado do nome do Servidor de Administração necessário.
   - No menu principal, vá para **Ativos (dispositivos)** → **Políticas e perfis** e clique no link de uma política.

2. Na janela aberta, vá para **Configuração de eventos**.

3. Clique em **Marcar exportação para o sistema SIEM usando o Syslog**.

Além disso, você pode marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, aberta ao se clicar no link do evento.

4. O sinal de verificação (✓) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.

A partir de agora, o Servidor de Administração envia os eventos marcados para o sistema SIEM se a exportação para o sistema SIEM estiver configurada.

Sobre a exportação de eventos usando o formato Syslog

Você pode usar o formato Syslog para exportar aos sistemas SIEM os eventos que ocorrem no Servidor de Administração e em outros aplicativos Kaspersky instalados em dispositivos gerenciados.

Syslog é um padrão para o protocolo de registro da mensagem. Isso permite a separação do software que gera mensagens, o sistema que as armazena e o software que os reporta e os analisa. Cada mensagem é legendada com um código de instalação, indicando o tipo de software que gera a mensagem e à mesma é atribuído um nível de gravidade.

O formato Syslog é definido por documentos de Solicitação de Comentários (RFC) publicados pela Internet Engineering Task Force (padrões da Internet). O padrão RFC 5424 é utilizado para exportar os eventos do Kaspersky Security Center Cloud Console aos sistemas externos.

No Kaspersky Security Center Cloud Console, você pode configurar a exportação dos eventos aos sistemas externos usando o formato Syslog.

O processo de exportação consistem em duas etapas:

1. Ativar a exportação automática do evento. Nesta etapa, o Kaspersky Security Center Cloud Console é configurado para que ele envie eventos ao sistema SIEM. O Kaspersky Security Center Cloud Console começa a enviar eventos imediatamente após você ativar a exportação automática.

2. Selecionar os eventos a ser exportados ao sistema externo. Nesta etapa, você seleciona qual evento exportar ao sistema SIEM.

Configurando o Kaspersky Security Center Cloud Console para exportação de eventos para o sistema SIEM

Para exportar eventos para o sistema SIEM, você deve configurar o processo de exportação no Kaspersky Security Center Cloud Console.

Para configurar a exportação para sistemas SIEM no Kaspersky Security Center Cloud Console:

1. No menu principal, clique no ícone de configurações (⚙) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **SIEM**.

3. Clique no link **Configurações**.

   A seção **Exportar as configurações** é aberta.

4. Especifique as configurações na seção **Exportar as configurações**:

   - **Endereço do servidor do sistema SIEM**

     O endereço IP do servidor onde o sistema SIEM atualmente usado está instalado. Verifique este valor nas suas configurações de sistema SIEM.

   - **Porta do sistema SIEM**

     O número da porta usada para estabelecer a conexão entre o Kaspersky Security Center Cloud Console e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center Cloud Console e nas configurações do receptor do seu sistema SIEM.

   - **Protocolo**

Você pode usar apenas o protocolo TLS sobre TCP para transferir mensagens para o sistema SIEM. Para fazer isso, especifique as configurações de TLS:

- **Autenticação do servidor**

  No campo **Autenticação do servidor**, você pode selecionar os valores de **Certificados confiáveis** ou de **Impressões digitais SHA**:

  - **Certificados confiáveis**. Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação (CA) confiável e carregá-lo no Kaspersky Security Center Cloud Console. O Kaspersky Security Center Cloud Console verifica se o certificado do servidor do sistema SIEM também é ou não assinado por um CA confiável.

    Para adicionar um certificado confiável, clique no botão **Procurar arquivo de certificados CA** e, em seguida, carregue o certificado.

  - **Impressões digitais SHA**. Você pode especificar as impressões digitais SHA-1 dos certificados do sistema SIEM no Kaspersky Security Center Cloud Console. Para adicionar uma impressão digital SHA-1, insira-a no campo **Impressões digitais** e, em seguida, clique no botão **Adicionar**.

  Ao usar a configuração **Adicionar autenticação do cliente**, você pode gerar um certificado para autenticar o Kaspersky Security Center Cloud Console. Assim, você usará um certificado autoassinado emitido pelo Kaspersky Security Center Cloud Console. Nesse caso, você pode usar um certificado confiável e uma impressão digital SHA para autenticar o servidor do sistema SIEM.

- **Adicionar nome do assunto/Nome alternativo do assunto**

  Nome do assunto é um nome de domínio para o qual o certificado foi recebido. O Kaspersky Security Center Cloud Console não poderá se conectar ao servidor do sistema SIEM se o nome de domínio dele não corresponder ao nome da entidade do certificado do servidor do sistema SIEM. No entanto, o servidor do sistema SIEM pode alterar seu nome de domínio se o nome tiver sido alterado no certificado. Neste caso, você pode especificar nomes de assuntos no campo **Adicionar nome do assunto/Nome alternativo do assunto**. Se qualquer um dos nomes de assunto especificados corresponder ao nome do assunto do certificado do sistema SIEM, o Kaspersky Security Center Cloud Console validará o certificado do servidor do sistema SIEM.

- **Adicionar autenticação do cliente**

  Para autenticação de cliente, você pode inserir o seu certificado ou gerá-lo no Kaspersky Security Center Cloud Console.

  - **Inserir certificado**. Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer CA confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

    - **Certificado X.509 PEM**. Carregue um arquivo com um certificado no campo **Arquivo com certificado** e um arquivo com uma chave privada no campo **Arquivo com chave**. Ambos os arquivos não dependem um do outro e a ordem de carregamento dos arquivos não é significativa. Quando os dois arquivos forem carregados, especifique a senha para decodificar a chave privada no campo **Verificação de senha ou certificado**. A senha pode ter um valor vazio se a chave privada não estiver codificada.

    - **Certificado X.509 PKCS12**. Carregue um único arquivo que contenha um certificado e sua chave privada no campo **Arquivo com certificado**. Quando o arquivo for carregado, especifique a senha para decodificar a chave privada no campo **Verificação de senha ou certificado**. A senha pode ter um valor vazio se a chave privada não estiver codificada.

- **Gerar chave**. Você pode gerar um certificado autoassinado no Kaspersky Security Center Cloud Console. Como resultado, o Kaspersky Security Center Cloud Console armazena o certificado autoassinado gerado e você pode passar a parte pública do certificado ou a impressão digital SHA1 para o sistema SIEM.

5. Se desejar, você pode exportar eventos arquivados do banco de dados do Servidor de Administração e definir a data de início da exportação de eventos arquivados:

   a. Clique no link **Definir a data de início da exportação**.

   b. Na seção aberta, especifique a data de início no campo **Data para início da exportação**.

   c. Clique no botão **OK**.

6. Alterne a opção para a posição **Exportar automaticamente os eventos para o banco de dados do sistema SIEM Ativado**.

7. Para verificar se a conexão do sistema SIEM foi configurada com êxito, clique no botão **Verificar conexão**.

   O status da conexão será exibido.

8. Clique no botão **Salvar**.

A exportação para o sistema SIEM está configurada. A partir de agora, se você configurou o recebimento de eventos em um sistema SIEM, o Servidor de Administração exportará os eventos marcados para um sistema SIEM. Se você definir a data de início da exportação, o Servidor de Administração também exportará os eventos marcados armazenados no banco de dados do Servidor de Administração a partir da data especificada.

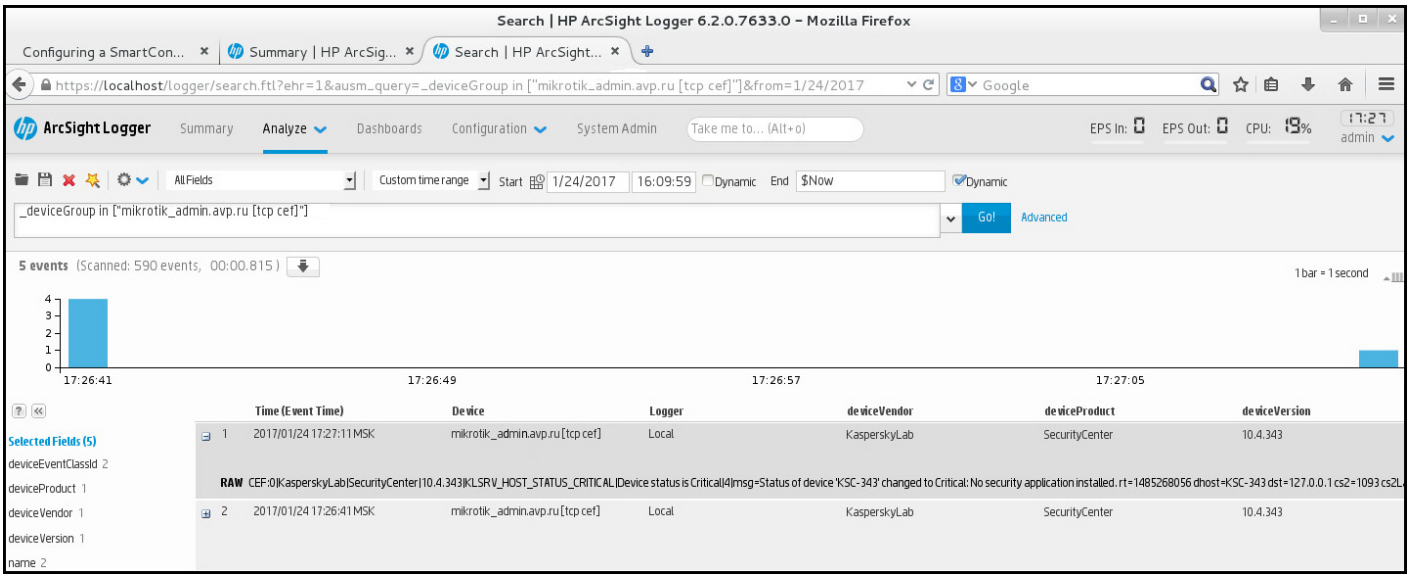
Exibir os resultados da exportação

Você pode controlar para a conclusão bem-sucedida do procedimento de exportação de eventos. Para fazer isto, verifique se as mensagens com eventos exportados são recebidas pelo seu sistema SIEM.

Se os eventos enviados do Kaspersky Security Center Cloud Console forem recebidos e apropriadamente analisados pelo seu sistema SIEM, a configuração nos dois lados foi feita apropriadamente. De outra forma, verifique as configurações que você especificou no Kaspersky Security Center Cloud Console contra a configuração no seu sistema SIEM.

A figura abaixo mostra os eventos exportados ao ArcSight. Por exemplo, o primeiro evento é crítico do Servidor de Administração: "*Status do dispositivo é crítico*".

A representação da exportação de eventos no sistema SIEM varia de acordo com o sistema SIEM que você usa.



Exemplo de eventos

Manual de Início Rápido para Provedores de Serviços Gerenciados (MSPs)

Este Manual de Início Rápido destina-se a administradores de Provedores de Serviços Gerenciados (MSPs).

O Kaspersky Security Center Cloud Console é compatível com multilocação. O guia contém dicas e melhores práticas para gerenciar as contas de seus clientes (locatários) e instalar os aplicativos de segurança nos dispositivos deles.

Sobre o Kaspersky Security Center Cloud Console

O Kaspersky Security Center Cloud Console é um aplicativo hospedado e mantido pela Kaspersky. Não é necessário instalar o Kaspersky Security Center Cloud Console em seu computador ou servidor. O Kaspersky Security Center Cloud Console permite que o administrador instale aplicativos de segurança da Kaspersky em dispositivos em uma rede corporativa, execute remotamente tarefas de verificação e atualização e gerencie as políticas de segurança dos aplicativos gerenciados. O administrador pode usar um painel detalhado que fornece uma visão instantânea do status de dispositivos corporativos, relatórios detalhados e configurações granulares nas políticas de proteção.

Principais recursos do Kaspersky Security Center Cloud Console

O Kaspersky Security Center Cloud Console permite que você faça o seguinte:

- Instalar aplicativos da Kaspersky em dispositivos em sua rede e gerenciar os aplicativos instalados.
- Crie uma hierarquia de grupos de administração para gerenciar uma seleção de dispositivos cliente como um todo.
- Crie Servidores de Administração virtuais e organize-os hierarquicamente.
- Proteja seus dispositivos de rede, incluindo estações de trabalho e servidores:
  - Gerencie um sistema de proteção antimalware integrado aos aplicativos Kaspersky.
  - Use os recursos de detecção e resposta (EDR e MDR) (é necessária uma licença para o Kaspersky Endpoint Detection and Response e/ou para Kaspersky Managed Detection and Response), incluindo:
    - Análise e investigação de incidentes
    - Visualização de incidentes por meio da criação de um gráfico da cadeia de desenvolvimento de ameaças
    - Aceite ou recusa manual de respostas ou configuração de aceitação automática de todas as respostas
- Use o Kaspersky Security Center Cloud Console como um aplicativo multi-tenant.
- Gerencie remotamente os aplicativos da Kaspersky instalados nos dispositivos clientes.
- Realize a implementação centralizada de chaves de licença para aplicativos da Kaspersky nos dispositivos cliente.
- Crie e gerencie políticas de segurança para dispositivos em sua rede.

- Crie e gerencie contas de usuário.
- Crie e gerencie funções de usuário (RBAC).
- Crie e gerencie tarefas para aplicativos instalados em dispositivos na rede.
- Visualize relatórios sobre o status do sistema de segurança para cada organização cliente individualmente.

Sobre o licenciamento do Kaspersky Security Center Cloud Console para MSPs

Ao começar a usar o Kaspersky Security Center Cloud Console, é possível solicitar um espaço de trabalho de avaliação (nesse caso, receberá uma licença de avaliação de 30 dias incorporada ao seu espaço de trabalho) ou inserir um código de ativação para uma licença comercial.

Não é possível converter um espaço de trabalho de avaliação em um comercial. Para continuar usando o Kaspersky Security Center Cloud Console após o término da licença de avaliação, será necessário excluir o espaço de trabalho de avaliação e criar outro com uma licença comercial.

Posteriormente, será possível adicionar uma ou várias chaves de licença comerciais ao repositório do Servidor de Administração.

Sobre os recursos de detecção e resposta para MSPs

O Kaspersky Security Center Cloud Console pode integrar recursos de outros aplicativos Kaspersky na interface do console. Por exemplo, você pode adicionar os recursos de detecção e resposta à funcionalidade do Kaspersky Security Center Cloud Console, integrando os seguintes aplicativos:

- Kaspersky Endpoint Detection and Response Optimum

  O Kaspersky Endpoint Detection and Response Optimum é uma solução projetada para proteger a infraestrutura de TI de uma organização contra ciberameaças complexas. A funcionalidade da solução combina a detecção automática de ameaças com a capacidade de responder a essas ameaças para resistir a ataques complexos, incluindo novos exploits, ransomware, ataques sem arquivo e métodos que usam ferramentas legítimas de sistema.

  Depois que um aplicativo Kaspersky Endpoint Protection Platform (EPP) detecta um incidente de segurança, um cartão detalhado com dados importantes sobre o incidente de segurança é gerado no Kaspersky Security Center Cloud Console. O cartão de incidente é gerado por um dos seguintes aplicativos:

  - Kaspersky Endpoint Agent, é instalado junto com um aplicativo Kaspersky EPP
  - Kaspersky Endpoint Security 11.7.0 for Windows ou posterior, que possui a funcionalidade EDR Optimum integrada e não requer instalação adicional do Kaspersky Endpoint Agent

  Uma ficha de incidente permite analisar e investigar o incidente. Além disso, você pode visualizar o incidente, criando um gráfico da cadeia de desenvolvimento de ameaças. O gráfico descreve as fases de implementação do ataque detectado ao longo do tempo. O gráfico criado inclui informações sobre os módulos envolvidos no ataque e as ações realizadas por esses módulos.

Você também pode iniciar uma cadeia de ações de resposta: criar uma regra de prevenção de execução para um objeto não confiável; pesquisar incidentes semelhantes no grupo de dispositivos, com base nos indicadores de comprometimento (IOC) selecionados; isolar um objeto não confiável ou isolar um dispositivo comprometido da rede.

Para obter informações sobre a ativação do aplicativo, consulte a documentação do Kaspersky Endpoint Detection and Response Optimum.

Se integrado, este aplicativo adiciona a seção **Alertas** à interface do Kaspersky Security Center Cloud Console (**Monitoramento e relatórios** → **Alertas**).

- Kaspersky Managed Detection and Response

  O Kaspersky Managed Detection and Response oferece proteção ininterrupta contra o volume crescente de ameaças capazes de desviar das barreiras de segurança automatizadas, sobrecarregando organizações que sofrem com a escassez de profissionais experientes ou que contam com recursos internos limitados. Os analistas de MDR SOC da Kaspersky ou de uma empresa terceirizada investigam os incidentes e oferecem soluções de resposta. Você pode aceitar ou rejeitar as medidas oferecidas manualmente, ou habilitar a opção de aceitar automaticamente todas as respostas.

  Para obter informações sobre a ativação do aplicativo, consulte a documentação de Kaspersky Managed Detection and Response.

  Se integrado, este aplicativo adiciona a seção **Incidentes** à interface do Kaspersky Security Center Cloud Console (**Monitoramento e relatórios** → **Incidentes**).

Você pode mostrar ou ocultar os elementos da interface, referentes aos recursos Kaspersky Endpoint Detection and Response ou Kaspersky Managed Detection and Response a qualquer momento n a seção **Opções da interface** do Kaspersky Security Center Cloud Console.

Guia de Introdução ao Kaspersky Security Center Cloud Console

Depois de concluir o cenário nesta seção, o Kaspersky Security Center Cloud Console estará pronto para uso.

Cenário do Guia de Introdução

O cenário continua em estágios:

1. **Criar uma conta**

   Para começar a usar o Kaspersky Security Center Cloud Console, é necessário ter uma conta.

   Para criar uma conta:

   1. Abra seu navegador e digite o seguinte endereço: https://ksc.kaspersky.com.
   2. Clique no botão **Criar uma conta**.
   3. Siga as instruções apresentadas na tela.

2. **Criar um espaço de trabalho**

   Após criar a conta, é possível registrar sua empresa e criar seu espaço de trabalho.

   Ao começar a usar o Kaspersky Security Center Cloud Console, é possível solicitar um espaço de trabalho de avaliação (nesse caso, receberá uma licença de avaliação de 30 dias incorporada ao seu espaço de trabalho) ou inserir um código de ativação para uma licença comercial.

Não é possível converter um espaço de trabalho de avaliação em um comercial. Para continuar usando o Kaspersky Security Center Cloud Console após o término da licença de avaliação, será necessário excluir o espaço de trabalho de avaliação e criar outro com uma licença comercial.

Para registrar uma empresa e criar um espaço de trabalho:

1. Abra seu navegador e digite o seguinte endereço: https://ksc.kaspersky.com.
2. Clique no botão **Login**.
3. Siga as instruções apresentadas na tela.

3. **Executar a configuração inicial do Kaspersky Security Center Cloud Console**

   Ao fazer login no espaço de trabalho criado pela primeira vez, automaticamente é solicitada a execução do Assistente de início rápido. O Assistente de início rápido orienta na criação de um conjunto mínimo de tarefas e políticas necessárias, na definição de uma configuração mínima e no início da criação de pacotes de instalação de aplicativos da Kaspersky. Siga as instruções apresentadas na tela.

Quando a configuração inicial estiver concluída, o Kaspersky Security Center Cloud Console estará pronto para uso.

Recomendações sobre como gerenciar os dispositivos de seus clientes

Esta seção contém recomendações para organizar os dispositivos de seus clientes que você deseja proteger.

As recomendações dependem do usuário estar utilizando o Kaspersky Security Center pela primeira vez ou já ter utilizado a versão local:

- Se você nunca usou a versão local do Kaspersky Security Center, terá duas opções:
  - Crie um Servidor de Administração virtual para os dispositivos de cada cliente (opção recomendada). Nesse caso, os dispositivos de cada cliente podem ser gerenciados por meio de um Servidor de Administração virtual dedicado, independentemente. Ao mesmo tempo, você pode usar o Servidor de Administração principal para criar políticas e tarefas comuns para todos os clientes. Os relatórios gerados no Servidor de Administração principal podem incluir dados de todos os Servidores de Administração virtuais.
  - Crie um grupo de administração para cada um de seus clientes. Se quiser dividir ainda mais os dispositivos dos clientes, poderá criar uma hierarquia de grupos de administração subordinados em cada grupo principal. Por exemplo, você pode precisar de grupos subordinados se quiser usar configurações de proteção diferentes para dispositivos de funcionários que trabalham em departamentos diferentes.
- Se você já usou o Kaspersky Security Center localmente, pode migrar os grupos de administração existentes e objetos relacionados do Kaspersky Security Center local para o Kaspersky Security Center Cloud Console.

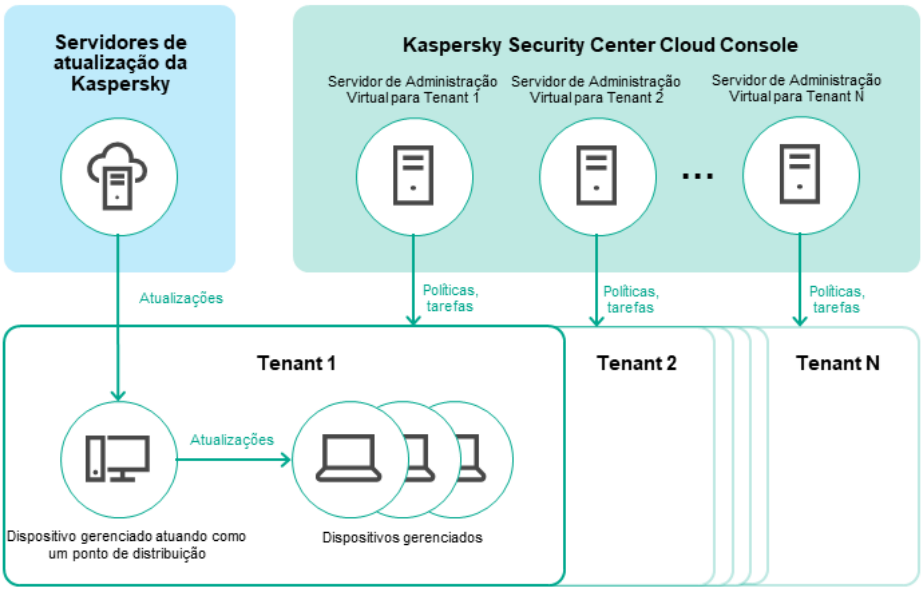
  Você não pode migrar Servidores de Administração virtuais. Depois de migrar os grupos de administração e outros objetos, você pode criar servidores de administração virtuais no Kaspersky Security Center Cloud Console.

  Prosseguir para a configuração da migração.

O administrador de um Servidor de Administração virtual só pode prosseguir para este Servidor virtual via Servidor de Administração principal. Todos os objetos criados no Servidor de Administração principal estão disponíveis para serem lidos pelo administrador de um Servidor de Administração virtual (por exemplo, widgets, relatórios ou funções de usuário).

Esquema de implementação típico para MSPs

Esta seção fornece uma descrição do esquema de implementação normalmente usado por MSPs para gerenciar vários locatários. O esquema é baseado no gerenciamento por meio de Servidores de Administração virtuais criados individualmente para cada tenant.



Esquema de implementação típico para MSPs

O esquema compreende os seguintes componentes principais:

- *Kaspersky Security Center Cloud Console*. Fornece uma interface de usuário para os serviços de administração do seu espaço de trabalho. Você usa o Kaspersky Security Center Cloud Console para implementar, gerenciar e manter o sistema de proteção de uma rede corporativa do cliente.
- *Servidores de atualização Kaspersky*. Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.
- *Servidores de Administração virtual*. Um administrador MSP normalmente cria um Servidor de Administração virtual para cada tenant para implementar, gerenciar e manter o sistema de proteção da rede da organização cliente correspondente.
- *Locatários*. Organizações dos clientes cujos dispositivos devem ser protegidos.
- *Dispositivos gerenciados*. Dispositivos da empresa cliente protegidos usando o Kaspersky Security Center Cloud Console. Cada dispositivo que precisa ser protegido deve ter o Agente de Rede e um dos aplicativos de segurança Kaspersky instalados.
- *Dispositivo gerenciado funcionando como um ponto de distribuição*. Um computador que tenha o Agente de Rede instalado e que é usado para a distribuição de atualizações, sondagem de rede, instalação remota de aplicativos, obtenção de informações sobre os computadores em um grupo de administração e/ou domínio de difusão. O administrador seleciona os dispositivos apropriados e atribui a eles pontos de distribuição manualmente.

Cenário: Implementação de proteção (gerenciamento de locatários usando Servidores de Administração virtuais)

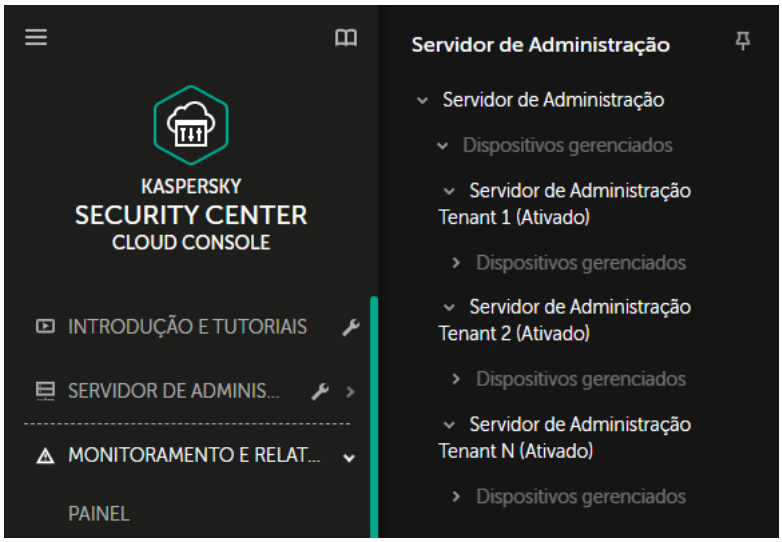
Se você nunca usou o Kaspersky Security Center e deseja gerenciar seus tenants por meio de Servidores de Administração virtuais, proceda conforme descrito nesta seção. Depois de concluir este cenário, os dispositivos de seus clientes estarão protegidos.

Se você gerencia vários tenants, execute o cenário para cada um deles separadamente.

O cenário continua em estágios:

1. **Criar um Servidor de Administração virtual**

   Crie um Servidor de Administração virtual para seu cliente. O novo Servidor de Administração virtual é exibido na hierarquia dos Servidores de Administração:



   Servidores de Administração Virtual na hierarquia de Servidores de Administração

2. **Selecionando um dispositivo para agir como ponto de distribuição**

   Entre os dispositivos do cliente, decida qual dispositivo atuará como um ponto de distribuição.

   > Não é possível ter mais de 100 pontos de distribuição em um espaço de trabalho.

3. **Criar um pacote de instalação independente para o Agente de Rede**

   Mude para o Servidor de Administração virtual criado e crie um pacote de instalação independente para o Agente de Rede. Você pode alternar os Servidores de Administração no menu principal, clicando no ícone de seta dupla (») à direita do nome do Servidor de Administração atual. Depois, selecione o Servidor de Administração necessário. Durante a criação do pacote de instalação independente, especifique o grupo de administração de dispositivos gerenciados para o qual migrar o dispositivo.

4. **Instalar o Agente de Rede no dispositivo selecionado para atuar como um ponto de distribuição**

   Você pode usar qualquer método que seja adequado para você:

   - Instalação manual

     Para fornecer o pacote de instalação independente ao dispositivo, é possível, por exemplo, copiá-lo para uma unidade removível (como um dispositivo USB) ou colocá-lo em uma pasta compartilhada.

- Implementação usando o Active Directory
- Implementação usando sua solução de software de monitoramento e gerenciamento remoto (RMM)

5. **Atribuindo os pontos de distribuição**

   Atribuir o dispositivo com o Agente de Rede instalado para atuar como um ponto de distribuição.

6. **Sondagem da rede**

   Configurar e executar uma sondagem de rede por meio de um ponto de distribuição.

   O Kaspersky Security Center Cloud Console oferece os seguintes métodos de sondagem da rede:

   - Sondagem do conjunto de IPs
   - Sondagem da rede do Windows
   - Sondagem do Active Directory

   Após a sondagem da rede ter sido concluída de acordo com o agendamento, os dispositivos de seus clientes são descobertos e colocados no grupo **Dispositivos não atribuídos**.

7. **Mover os dispositivos descobertos para os grupos de administração**

   Configure as regras para migrar os dispositivos descobertos automaticamente para os grupos de administração necessários ou migre esses dispositivos para os grupos de administração necessários manualmente. Se você planeja gerenciar os dispositivos do cliente em um único grupo de administração, pode migrar os dispositivos para o grupo dispositivos gerenciados.

8. **Criando pacotes de instalação para o Agente de Rede e os aplicativos gerenciados Kaspersky**

   Crie pacotes de instalação para aplicativos da Kaspersky.

9. **Removendo aplicativos de segurança de terceiros**

   Se aplicativos de segurança de terceiros estiverem instalados nos dispositivos de seus clientes, remova-os antes de instalar os aplicativos Kaspersky.

10. **Instalando aplicativos Kaspersky em dispositivos cliente**

    Crie tarefas de instalação remota para instalar o Agente de Rede e os aplicativos Kaspersky gerenciados nos dispositivos de seus clientes.

    Se necessário, você também pode criar várias tarefas de instalação remota para instalar aplicativos gerenciados da Kaspersky para diferentes grupos de administração ou seleções de dispositivos diferentes.

    Após a criação das tarefas, você pode definir as suas configurações. Certifique-se de que o agendamento de cada tarefa atenda aos seus requisitos. Primeiro, a tarefa para instalar o Agente de Rede deve ser executada. Após a instalação do Agente de Rede nos dispositivos de seus clientes, a tarefa para instalar os aplicativos gerenciados da Kaspersky deve ser executada.

11. **Verificando a implementação inicial dos aplicativos Kaspersky**

    Gere e visualize o **Relatório de versões de software da Kaspersky**. Verifique se os aplicativos gerenciados da Kaspersky estão instalados em todos os dispositivos dos clientes.

12. **Criando políticas para aplicativos Kaspersky**

    Crie uma política para o aplicativo Kaspersky necessário. Se você deseja criar uma política universal para todos os clientes, troque o Servidor de Administração virtual atual para o Servidor de Administração principal e depois crie uma política para o aplicativo Kaspersky necessário.

Cenário: implementação de proteção (gerenciamento de tenants por meio de grupos de administração)

Se você nunca usou o Kaspersky Security Center e deseja gerenciar seus tenants por meio de grupos de administração, proceda conforme descrito nesta seção. Depois de concluir este cenário, os dispositivos de seus clientes estarão protegidos.

O cenário continua em estágios:

1. **Criação de grupos de administração**

   Criar um grupo de administração para cada um de seus clientes.

2. **Planejando a estrutura dos pontos de distribuição**

   Entre os dispositivos de cada cliente, decida qual dispositivo atuará como um ponto de distribuição.

   > Não é possível ter mais de 100 pontos de distribuição em um espaço de trabalho.

3. **Criar um pacote de instalação independente para o Agente de Rede**

   Criando um pacote de instalação independente para o Agente de Rede.

4. **Instalação do Agente de Rede no dispositivo selecionado para atuar como um ponto de distribuição**

   Instalar o Agente de Rede nos dispositivos selecionados para atuar como pontos de distribuição.

   Você pode usar qualquer método que seja adequado para você:

   - Instalação manual

     Para entregar o pacote de instalação independente aos dispositivos, é possível, por exemplo, copiá-lo para uma unidade removível (como um pendrive) ou colocá-lo em uma pasta compartilhada.

   - Implementação usando o Active Directory
   - Implementação usando sua solução de software de monitoramento e gerenciamento remoto (RMM)

5. **Atribuir os pontos de distribuição**

   Atribuir o dispositivo com o Agente de Rede instalado para atuar como pontos de distribuição.

6. **Sondagem da rede**

   Configurar e executar uma sondagem de rede por meio de um ponto de distribuição.

   O Kaspersky Security Center Cloud Console oferece os seguintes métodos de sondagem da rede:

   - Sondagem do conjunto de IPs
   - Sondagem da rede do Windows
   - Sondagem do Active Directory

   Após a sondagem da rede ter sido concluída de acordo com o agendamento, os dispositivos de seus clientes são descobertos e colocados no grupo **Dispositivos não atribuídos**.

7. **Mover os dispositivos descobertos para os grupos de administração**

Configure as regras para migrar os dispositivos descobertos automaticamente para os grupos de administração necessários ou migre esses dispositivos para os grupos de administração necessários manualmente.

8. **Criando pacotes de instalação para o Agente de Rede e os aplicativos gerenciados Kaspersky**

   Caso não tenha iniciado o Assistente de Início Rápido ou tenha ignorado a etapa de criação de pacotes de instalação, crie pacotes de instalação para os aplicativos Kaspersky.

9. **Removendo aplicativos de segurança de terceiros**

   Se aplicativos de segurança de terceiros estiverem instalados nos dispositivos de seus clientes, remova-os antes de instalar os aplicativos Kaspersky.

10. **Instalando os aplicativos Kaspersky nos dispositivos dos seus clientes**

    Crie tarefas de instalação remota para instalar o Agente de Rede e os aplicativos Kaspersky gerenciados nos dispositivos de seus clientes.

    Se necessário, você também pode criar várias tarefas de instalação remota para instalar aplicativos gerenciados da Kaspersky para diferentes grupos de administração ou seleções de dispositivos diferentes.

    Após a criação das tarefas, você pode definir as suas configurações. Certifique-se de que o agendamento de cada tarefa atenda aos seus requisitos. Primeiro, a tarefa para instalar o Agente de Rede deve ser executada. Após a instalação do Agente de Rede nos dispositivos de seus clientes, a tarefa para instalar os aplicativos gerenciados da Kaspersky deve ser executada.

11. **Verificando a implementação inicial dos aplicativos Kaspersky**

    Gere e visualize o **Relatório de versões de software da Kaspersky**. Verifique se os aplicativos gerenciados da Kaspersky estão instalados em todos os dispositivos de seus clientes.

12. **Criando políticas para aplicativos Kaspersky**

    Acesse o menu **Ativos (dispositivos)** → **Grupos**; caso queira criar uma política universal para todos os clientes, selecione **servidor de administração.** Se você deseja criar uma política específica para um cliente individual, selecione o grupo de administração correspondente a esse cliente. Crie uma política para o aplicativo Kaspersky necessário.

Uso conjunto do Kaspersky Security Center local e do Kaspersky Security Center Cloud Console

Se você já usou o Kaspersky Security Center executado no local, poderá converter os Servidores de Administração existentes em execução em Servidores de Administração secundários do seu novo Servidor de Administração do Kaspersky Security Center Cloud Console, conforme descrito nesta seção.

Se você configurar o uso conjunto do Kaspersky Security Center local e do Kaspersky Security Center Cloud Console, não poderá migrar do Kaspersky Security Center local para o Kaspersky Security Center Cloud Console, a menos que remova a hierarquia dos Servidores de Administração.

Para criar uma hierarquia de Servidores de Administração,

Adicione os Servidores de Administração existentes executados no local como Servidores de Administração secundários.

Licenciando aplicativos Kaspersky para MSPs

O Kaspersky Security Center Cloud Console permite realizar a distribuição centralizada de chaves de licença para os aplicativos Kaspersky nos dispositivos dos clientes, monitorar o uso e renovar licenças.

Se você gerencia vários tenants, pode distribuir as chaves de licença das seguintes maneiras:

- Uma chave de licença para todos os tenants.
- Uma chave de licença individual para cada tenant.

Para distribuir chaves de licença para os dispositivos de seus clientes:

1. Adicione a chave de licença necessária ao repositório do Servidor de Administração.
2. Execute uma das seguintes ações:
   - Configure a distribuição automática de uma chave de licença.

     Nesse caso, o Kaspersky Security Center Cloud Console seleciona uma das chaves de licença aplicáveis e a implanta automaticamente sempre que um novo dispositivo é descoberto.
   - Configure a tarefa Adicionar uma chave para distribuir uma chave de licença para os dispositivos.

     Ao configurar a tarefa, você seleciona a chave de licença que deve ser implantada nos dispositivos e o grupo de administração que contém os dispositivos necessários.

     Uma tarefa pode distribuir apenas uma chave de licença. Isso significa que, se você deseja distribuir várias chaves de licença, deve criar uma tarefa para cada uma delas.

Os aplicativos Kaspersky instalados nos dispositivos de seus clientes são ativados.

Monitorando e relatoriando recursos para MSPs

O Kaspersky Security Center Cloud Console fornece recursos de monitoramento e geração de relatórios. Esses recursos fornecem uma visão geral da infraestrutura da sua organização, dos status de proteção e das estatísticas.

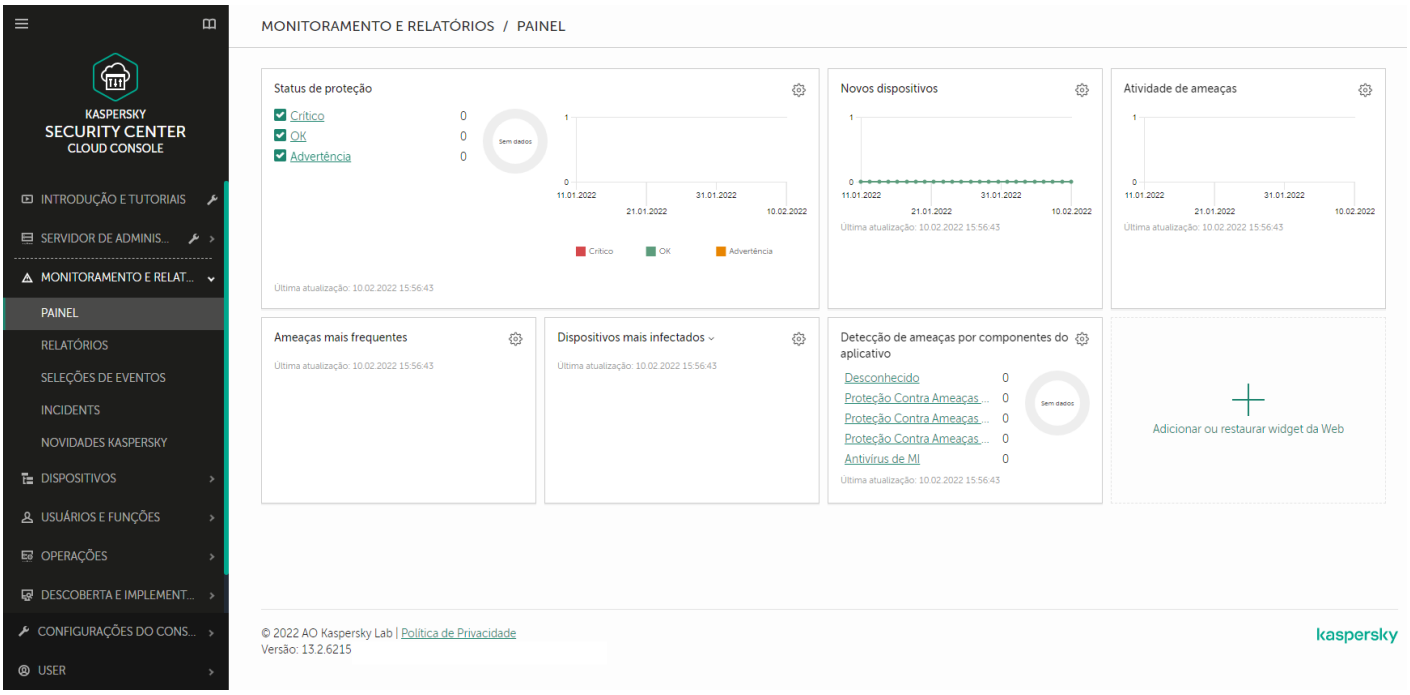
Quando você tiver implementado o Kaspersky Security Center Cloud Console, poderá configurar os recursos de monitoramento e relatórios para melhor atender às suas necessidades.

O Kaspersky Security Center Cloud Console fornece os seguintes tipos de recursos de monitoramento e relatório:

- Painel
- Relatórios
- Seleções de eventos
- Notificações por e-mail

Painel

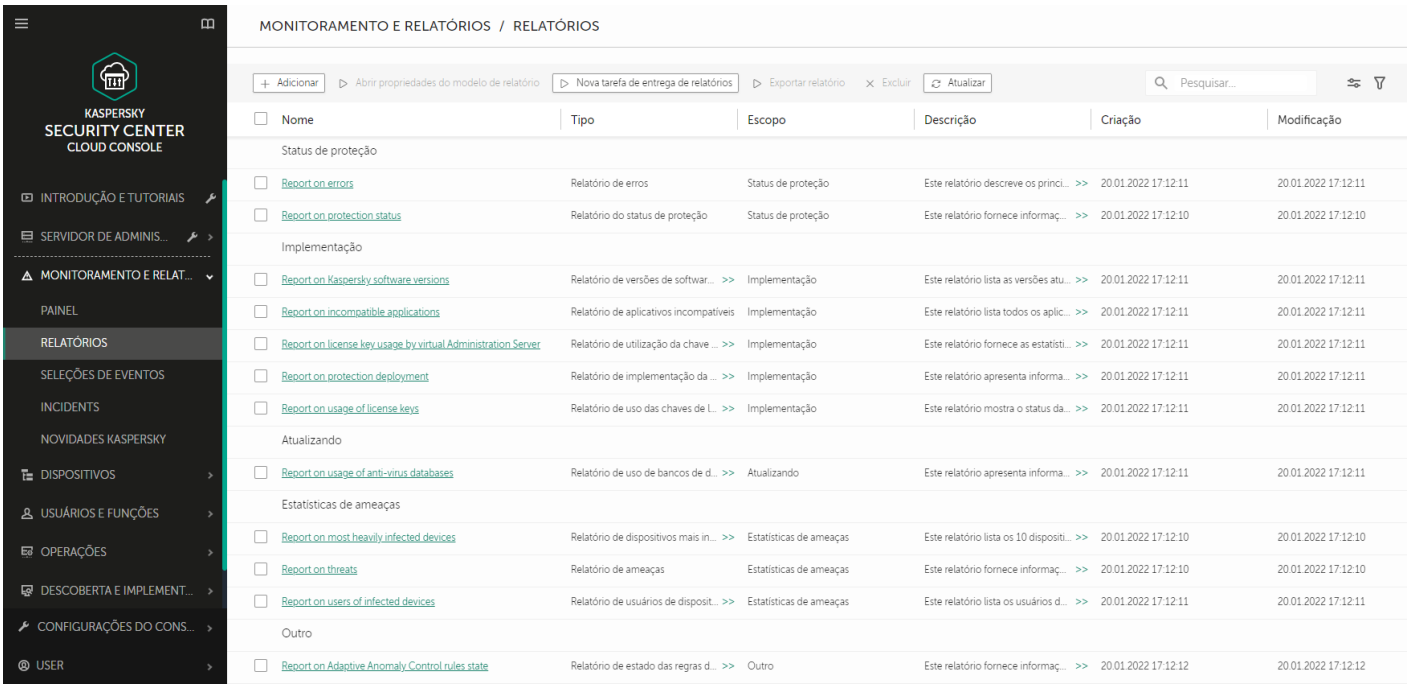
O painel permite monitorar tendências de segurança na rede da sua organização fornecendo uma exibição gráfica das informações. (Veja a figura abaixo).



A seção Painel

Relatórios

O recurso Relatórios permite obter informações numéricas detalhadas sobre a segurança da rede da sua organização, salvar essas informações em um arquivo, enviá-las por e-mail e imprimi-las. Você também pode agendar a entrega do relatório por e-mail (veja a figura abaixo).



A seção Relatórios

Seleções de eventos

As seleções de evento fornecem uma visualização na tela de conjuntos nomeados de eventos selecionados do banco de dados do Servidor de Administração. O Kaspersky Security Center Cloud Console contém várias seleções de eventos predefinidas (por exemplo, **Eventos recentes** e **Eventos críticos**). Além disso, você pode criar seleções de eventos personalizadas.

Notificações por e-mail

Você pode configurar a notificação por e-mail de eventos que ocorrem no Kaspersky Security Center Cloud Console.

Trabalhando com o Kaspersky Security Center Cloud Console em um ambiente em nuvem

Esta seção fornece informações sobre os recursos do Kaspersky Security Center Cloud Console relacionados à implementação e manutenção do Kaspersky Security Center Cloud Console em ambientes em nuvem, como Amazon Web Services, Microsoft Azure ou Google Cloud.

Para trabalhar em um ambiente em nuvem, é necessária uma licença especial. Se você não tiver essa licença, os elementos da interface relacionados aos dispositivos na nuvem não funcionarão.

Opções de licenciamento em um ambiente em nuvem

Trabalhar em um ambiente de nuvem é possível no modo de teste e no modo comercial do Kaspersky Security Center Cloud Console:

- No modo de teste, todos os recursos do ambiente de nuvem estão disponíveis durante todo o período de validade do espaço de trabalho. Nenhuma licença é necessária.
- No modo comercial, os recursos do ambiente de nuvem estão disponíveis apenas se uma chave de licença do Kaspersky Hybrid Cloud Security tiver sido adicionada como ativa nas propriedades do Servidor de Administração.

Em ambos os casos, Gerenciamento de patches e vulnerabilidades é ativado automaticamente.

Você pode encontrar um erro ao tentar ativar o recurso de Suporte do ambiente em nuvem usando a licença do Kaspersky Hybrid Cloud Security.

Preparando-se para trabalhar em um ambiente de nuvem usando o Kaspersky Security Center Cloud Console

Esta seção informa como preparar-se para trabalhar com o Kaspersky Security Center Cloud Console no Amazon Web Services:

- Amazon Web Services
- Microsoft Azure
- Google Cloud

Trabalhando no ambiente de nuvem Amazon Web Services

Esta seção informa a você como preparar-se para trabalhar com o Kaspersky Security Center Cloud Console no Amazon Web Services.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center Cloud Console.

Sobre o trabalho no ambiente na nuvem de Amazon Web Services

Para trabalhar com a plataforma AWS e, especialmente, para criar instâncias, você precisa ter uma conta do Amazon Web Services. Você pode criar uma conta gratuita em https://aws.amazon.com. Você também pode usar uma conta existente da Amazon.

Para saber mais sobre uma AMI e como funciona o AWS Marketplace, visite a página de Ajuda do AWS Marketplace. Para obter mais informações sobre o trabalho com a plataforma de AWS, usando instâncias e conceitos relacionados, consulte a documentação de Amazon Web Services.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center Cloud Console.

Criando contas de Usuário do IAM para instâncias do Amazon EC2

Esta seção descreve as ações que devem ser realizadas para assegurar a operação correta do Kaspersky Security Center Cloud Console. Estas ações incluem trabalhar com as contas de usuário e funções do AWS Identity And Access Management (IAM). Também estão descritas as ações que devem ser tomadas nos dispositivos cliente para instalar o Agente de Rede nos dispositivos e instalar o Kaspersky Security for Windows Server e o Kaspersky Endpoint Security for Linux.

Certificando-se que o Kaspersky Security Center Cloud Console tenha as permissões para trabalhar com AWS

Para operar no ambiente de nuvem do Amazon Web Services usando o console de nuvem do Kaspersky Security Center, você deve criar uma *conta de usuário IAM*, que será usada pelo Kaspersky Security Center Cloud Console para trabalhar com serviços AWS. Antes de começar a trabalhar com o Servidor de Administração, crie uma conta de Usuário do IAM com uma *chave de acesso AWS IAM* correspondente (aqui também referida como *chave de acesso IAM*).

A criação de uma conta de usuário do IAM requer o console de gerenciamento AWS. Para trabalhar com o Console de Gerenciamento AWS, você precisará de um nome do usuário e senha de uma conta no AWS.

Criar uma conta de Usuário do IAM para trabalhar com o Kaspersky Security Center Cloud Console

Uma conta de usuário IAM é necessária para trabalhar com o Kaspersky Security Center Cloud Console. Você pode criar uma conta de usuário IAM com todas as permissões necessárias, ou pode criar duas contas de usuário separadas.

Uma *chave de acesso IAM* que você terá que fornecer ao Kaspersky Security Center Cloud Console durante a configuração inicial é automaticamente criada para o Usuário do IAM. Uma chave de acesso IAM consiste em uma ID da chave de acesso e uma chave secreta. Para obter mais detalhes sobre mim o serviço IAM, consulte as seguintes páginas de referência AWS:

- https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- https://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Para criar uma conta de usuário IAM com as permissões necessárias:

1. Abra o Console de Gerenciamento AWS e efetue o login na sua conta.
2. Na lista de serviços AWS, selecione **IAM**.

   Uma janela é aberta contendo uma lista de nomes de usuários e um menu que permite a você trabalhar com a ferramenta.
3. Navegue pelas áreas do console processando as contas de usuário e adicione um novo nome de usuário ou mais.
4. Para o(s) usuário(s) você adicionar, especifique as seguintes propriedades do AWS:
   - Tipo de acesso: **Acesso programático**.
   - Limite de permissões não definido.
   - Permissão: **ReadOnlyAccess**.

     Após adicionar a permissão, visualize-as para confirmar a exatidão. Em caso de uma seleção por engano, volte à tela anterior e faça a seleção novamente.
5. Após criar a conta de usuário, uma tabela será exibida contendo a chave de acesso IAM do novo Usuário do IAM. A ID da chave de acesso é exibida na coluna **ID da chave de acesso**. A chave secreta é exibida como asteriscos na coluna **Chave de acesso secreta**. Para visualizar a chave secreta, clique em **Exibir**.

A conta recentemente criada é exibida na lista de contas de usuários IAM que correspondem à sua conta no AWS.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center Cloud Console.

Trabalhando no ambiente de nuvem Microsoft Azure

Esta seção fornece informações sobre a implementação a operação e manutenção do Kaspersky Security Center Cloud Console em um ambiente nuvem, fornecido pelo Microsoft Azure, assim como detalhes da implementação da proteção em máquinas virtuais neste ambiente nuvem.

Sobre o trabalho em o Microsoft Azure

Para trabalhar com a plataforma Microsoft Azure e, em particular, comprar aplicativos no Azure Marketplace e criar máquinas virtuais, você precisará de uma assinatura do Azure. Antes de começar a trabalhar com o Microsoft Azure no console de nuvem do Kaspersky Security Center Cloud Console, crie uma ID do aplicativo do Azure com as permissões necessárias para a instalação de aplicativos em máquinas virtuais.

Criar uma assinatura, ID do aplicativo e senha

Para trabalhar com o Kaspersky Security Center Cloud Console no ambiente do Microsoft Azure, você precisa de uma assinatura do Azure, uma ID do aplicativo Azure e a senha do aplicativo Azure. É possível usar uma assinatura existente, se você já tiver uma.

Uma assinatura do Azure concede ao proprietário acesso ao Portal de Gerenciamento da Plataforma Microsoft Azure e aos serviços do Microsoft Azure. O proprietário pode usar a Plataforma Microsoft Azure para gerenciar serviços como o Azure SQL e o Azure Storage.

Para criar uma assinatura do Microsoft Azure,

Vá para https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription e siga as instruções fornecidas.

Mais informações sobre como criar uma assinatura estão disponíveis no site da Microsoft. Você obterá uma ID de assinatura que, mais tarde, fornecerá ao Kaspersky Security Center Cloud Console em conjunto com a ID do aplicativo e a senha.

Para criar e salvar o ID do aplicativo Azure e a senha:

1. Acesse https://portal.azure.com e assegure-se de fazer login.
2. Seguindo as instruções na página de referência, crie seu ID do aplicativo.
3. Acesse a seção **Chaves** das configurações do aplicativo.
4. Na seção **Chaves**, preencha os campos **Descrição** e **Expira** e deixe o campo **Valor** em branco.
5. Clique em **Salvar**.

   Quando você clica **em Salvar**, o sistema preenche automaticamente o campo **Valor** com uma sequência de caracteres longa. Essa sequência é a sua senha do Aplicativo Azure (por exemplo, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QIfFvdU=). A descrição é exibida da forma como você a digitar.
6. Copie a senha e salve-a para depois fornecê-la, junto com a ID do aplicativo, ao Kaspersky Security Center Cloud Console.

   Você pode copiar a senha somente quando ela tiver sido criada. Mais tarde, a senha não será exibida e você não conseguirá restaurá-la.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center Cloud Console.

Atribuir uma função ao ID do aplicativo Azure

Se você quiser detectar máquinas virtuais usando descoberta de dispositivos, o ID do aplicativo Azure deverá ter a função Leitor. Se além de detectar, você quiser implementar a proteção através da API do Azure, sua ID do aplicativo Azure deve ter a função Virtual Machine Contributor.

Siga as instruções no site da Microsoft para atribuir uma função ao ID do aplicativo Azure.

Trabalhando no Google Cloud

Esta seção fornece informações sobre como trabalhar com o Kaspersky Security Center Cloud Console em um ambiente em nuvem fornecido pelo Google.

É possível usar o Google API para trabalhar com o Kaspersky Security Center Cloud Console na plataforma Google Cloud. É necessária uma conta do Google. Consulte a documentação do Google em https://cloud.google.com para obter mais informações.

Será necessário criar e fornecer ao Kaspersky Security Center Cloud Console as seguintes credenciais:

- **E-mail do cliente**

  O e-mail do cliente é o endereço usado para registrar o seu projeto no Google Cloud.

- **ID do projeto**

  O ID do projeto é o código recebido no ato do registro do seu projeto no Google Cloud.

- **Chave privada**

  A chave privada é a sequência de caracteres recebida como sua chave privada ao registrar o seu projeto no Google Cloud. Você pode copiar e colar esta sequência para evitar erros.

Assistente de configuração de ambiente em nuvem no Kaspersky Security Center Cloud Console

Para configurar o Kaspersky Security Center Cloud Console usando este assistente, você deve ter o seguinte:

- Credenciais específicas para um ambiente em nuvem:
  - A conta de usuário IAM que recebeu o direito de pesquisar o segmento de nuvem (para trabalhar com Amazon Web Services)
  - ID do Aplicativo Azure, senha e assinatura (para trabalhar com Microsoft Azure)
  - E-mail do cliente do Google, ID do projeto e chave privada (para trabalhar com o Google Cloud)
- Pacotes de instalação:
  - Agente de Rede para Windows
  - Agente de Rede para Linux

    - Kaspersky Endpoint Security for Linux
- Plug-in da Web para o Kaspersky Endpoint Security for Linux
- Pelo menos um dos seguintes itens:
    - Pacote de instalação e plug-in da Web para o Kaspersky Endpoint Security for Windows (recomendado)
    - O pacote de instalação e o plugin da Web para o Kaspersky Security for Windows Server

O assistente de configuração de ambiente em nuvem é iniciado automaticamente na primeira conexão com o Kaspersky Security Center Cloud Console se o espaço de trabalho foi criado usando a licença do Kaspersky Hybrid Cloud Security. Você também pode iniciar o assistente de configuração de ambiente em nuvem manualmente a qualquer momento.

Para iniciar manualmente o assistente de configuração do ambiente em nuvem:

No menu principal, acesse **Descoberta e implementação → Implementação e atribuição → Configurar ambiente em nuvem**.

O assistente é iniciado.

A duração média de uma sessão de trabalho com este assistente é de aproximadamente 15 minutos.

Etapa 1. Verificação dos plug-ins e pacotes de instalação necessários

Essa etapa não será exibida caso tenha todos os plug-ins da Web e pacotes de instalação necessários e listados abaixo.

Para configurar um ambiente na nuvem, é necessário ter os seguintes componentes:

- Pacotes de instalação:
    - Agente de Rede para Windows
    - Agente de Rede para Linux
    - Kaspersky Endpoint Security for Linux
- Plug-in da Web para o Kaspersky Endpoint Security for Linux
- Pelo menos um dos seguintes itens:
    - Pacote de instalação e plug-in da Web para o Kaspersky Endpoint Security for Windows (recomendado)
    - O pacote de instalação e o plugin da Web para o Kaspersky Security for Windows Server

      Recomendamos usar o Kaspersky Endpoint Security for Windows em vez do Kaspersky Security for Windows Server.

O Kaspersky Security Center Cloud Console detecta automaticamente os componentes possuídos e lista apenas os que estão faltando. Baixe os componentes listados clicando no botão **Selecionar os aplicativos para download** e, em seguida, selecione os plug-ins e pacotes de instalação necessários. Depois de baixar um componente, será possível usar o botão **Atualizar** para atualizar a lista de componentes ausentes.

Etapa 2. Selecionando o método de ativação do aplicativo

Esta etapa é exibida apenas se você usou uma licença diferente do Kaspersky Hybrid Cloud Security durante a criação do espaço de trabalho e nunca adicionou uma chave de licença do Kaspersky Hybrid Cloud Security ao campo de ativação do Servidor de Administração. Nesse caso, você deve ativar o Servidor de Administração usando uma licença do Kaspersky Hybrid Cloud Security.

Etapa 3. Seleção do ambiente em nuvem e autorização

Especificar as seguintes configurações:

- **Ambiente em nuvem**

  Selecione o ambiente em nuvem no qual você está implementando o Kaspersky Security Center Cloud Console: AWS, Azure ou Google Cloud.

  Caso planeje trabalhar com mais de um ambiente em nuvem, selecione um ambiente e execute o assistente novamente.

- **Nome da conexão**

  Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

  Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

  Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

Insira suas credenciais para receber autorização no ambiente em nuvem que especificou.

AWS

Se você selecionou AWS como tipo de segmento da nuvem, use uma chave de acesso AWS IAM para sondagem adicional do segmento da nuvem. Insira os seguintes dados de chave:

- **ID da chave de acesso**

  A ID da chave de acesso IAM é uma sequência de caracteres alfanuméricos. Você recebeu a ID da chave quando você criou a conta de usuário IAM.

  O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização.

- **Chave secreta**

A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização.

Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

Azure

Se você selecionou Azure como o tipo de segmento da nuvem, especifique as seguintes configurações para a conexão que será usada para sondagem adicional do segmento da nuvem:

- **ID do aplicativo Azure**

  Você criou este ID do aplicativo no portal do Azure.

  É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- **ID da assinatura do Azure**

  Você criou a assinatura no portal do Azure.

- **Senha do aplicativo Azure**

  Você recebeu a senha quando criou o ID do aplicativo.

  Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

- **Nome da conta de armazenamento do Azure**

  Você criou o nome da conta de armazenamento do Azure para trabalhar com o Kaspersky Security Center Cloud Console.

- **Chave de acesso ao armazenamento do Azure**

  Você recebeu uma senha (chave) quando criou a conta de armazenamento Azure para trabalhar com o Kaspersky Security Center Cloud Console.

  A chave está disponível na seção "Visão geral da conta de armazenamento Azure", na subseção "Chaves".

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

Google Cloud

Se você selecionou Google Cloud como o tipo de segmento da nuvem, especifique as seguintes configurações para a conexão que será usada para sondagem adicional do segmento da nuvem:

- **Endereço de e-mail do cliente**

  O e-mail do cliente é o endereço usado para registrar o seu projeto no Google Cloud.

- **ID do projeto**

  O ID do projeto é o código recebido no ato do registro do seu projeto no Google Cloud.

- **Chave privada**

  A chave privada é a sequência de caracteres recebida como sua chave privada ao registrar o seu projeto no Google Cloud. Você pode copiar e colar esta sequência para evitar erros.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

A conexão especificada é salva nas configurações do aplicativo.

O assistente de Configuração de ambiente em nuvem permite especificar apenas um segmento. Posteriormente, você poderá especificar mais conexões para gerenciar outros segmentos da nuvem.

Clique em **Avançar** para prosseguir.

Etapa 4. Sondagem de segmentos e configuração de sincronização com a nuvem

Neste passo, a sondagem de segmentos da nuvem é iniciada e um grupo de administração especial para dispositivos na nuvem é criado automaticamente. Os dispositivos detectados durante a sondagem são colocados neste grupo. O agendamento de sondagem de segmentos da nuvem é configurado a cada cinco minutos, por padrão (é possível alterar essa configuração posteriormente).

Uma regra automática para mover **Sincronizar com a Nuvem** também é criada. Para cada verificação subsequente da rede na nuvem, os dispositivos virtuais detectados serão movidos ao subgrupo correspondente dentro do grupo **Dispositivos gerenciados\Cloud**.

Defina a configuração **Sincronizar grupos de administração com estrutura de nuvem**.

Se essa opção é ativada, o grupo **Nuvem** é automaticamente criado dentro do grupo **Dispositivos gerenciados** e uma descoberta de dispositivos na nuvem é iniciada. As instâncias e máquinas virtuais detectadas durante cada verificação da rede na nuvem são colocadas no grupo Nuvem. A estrutura dos subgrupos de administração dentro deste grupo corresponde à estrutura do seu segmento da nuvem (no AWS, as zonas de disponibilidade e os grupos de posicionamento não são representados na estrutura; no Azure, as sub-redes não são representadas na estrutura). Os dispositivos que não foram identificados como instância no ambiente nuvem estão no grupo **Dispositivos não atribuídos**. Esta estrutura de grupo permite usar tarefas de instalação de grupo para instalar aplicativos antivírus nas instâncias, bem como definir políticas diferentes para grupos diferentes.

Se esta opção estiver desativada, o grupo **Nuvem** também será criado, e a descoberta de dispositivos de nuvem também será iniciada; contudo, os subgrupos que correspondem à estrutura do segmento da nuvem não serão criados no grupo. Todas as instâncias detectadas estão no grupo de administração **Nuvem**, portanto elas são exibidos em uma lista única. Se o seu trabalho com o Kaspersky Security Center Cloud Console precisar de sincronização, você pode modificar as propriedades da regra **Sincronizar com a nuvem** e forçá-la. Forçar esta regra alterará a estrutura dos subgrupos no grupo Nuvem para que ele coincida com a estrutura do seu segmento da nuvem.

Por padrão, esta opção está desativada.

Clique em **Avançar** para prosseguir.

Etapa 5. Seleção de um aplicativo para criar uma política e tarefas

Essa etapa só é exibida caso tenha pacotes de instalação e plug-ins para o Kaspersky Endpoint Security for Windows e o Kaspersky Security for Windows Server. Caso tenha um plug-in e um pacote de instalação para apenas um desses aplicativos, essa etapa será ignorada e o Kaspersky Security Center Cloud Console criará uma política e tarefas para o aplicativo existente.

Selecione um aplicativo para o qual deseja criar uma política e tarefas:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

Etapa 6. Configuração da Kaspersky Security Network para o Kaspersky Security Center Cloud Console

Este passo a é ignorado ao executar o Kaspersky Security Center Cloud Console no modo de avaliação ou em um Servidor de Administração virtual.

Especifique as configurações para encaminhar informações sobre as operações do Kaspersky Security Center Cloud Console à Base de conhecimento da Kaspersky Security Network (KSN). Selecione uma das seguintes opções:

- **Concordo em usar a Kaspersky Security Network**

  O Kaspersky Security Center Cloud Console e os aplicativos gerenciados instalados nos dispositivos cliente transferem automaticamente seus detalhes de operação para a Kaspersky Security Network. A participação na Kaspersky Security Network assegura atualizações mais rápidas dos bancos de dados que contêm informações sobre vírus e outras ameaças, que assegura uma resposta mais rápida a ameaças de segurança emergentes.

- **Não concordo em usar a Kaspersky Security Network**

O Kaspersky Security Center Cloud Console e os aplicativos gerenciados não fornecerão informações à Kaspersky Security Network.

Se você selecionar esta opção, o uso da Kaspersky Security Network será desativado.

A Kaspersky recomenda a participação na Kaspersky Security Network.

Os contratos da KSN para aplicativos gerenciados também podem ser exibidos. Se você concordar em usar a Kaspersky Security Network, o aplicativo gerenciado enviará dados para a Kaspersky. Se você não concordar em participar da Kaspersky Security Network, o aplicativo gerenciado não enviará dados para a Kaspersky. Você pode alterar esta configuração posteriormente na política do aplicativo.

Clique em **Avançar** para prosseguir.

Etapa 7. Criar uma configuração inicial de proteção

Você poderá verificar a lista de políticas e tarefas que foram criadas.

Aguarde a conclusão da criação de políticas e tarefas e, em seguida, clique em **Avançar** para prosseguir. Na última página do assistente, clique no botão **Concluir** para sair.

Sondando o segmento de rede com o Kaspersky Security Center Cloud Console

As informações sobre a estrutura da rede (e de seus dispositivos) são recebidas pelo segmentos da nuvem usando as ferramentas AWS API, Azure API ou Google API. O Kaspersky Security Center Cloud Console usa estas informações para atualizar o conteúdo das pastas Dispositivos não atribuídos e Dispositivos gerenciados. Se você tiver configurado dispositivos a ser movidos automaticamente para grupos de administração, os dispositivos detectados são incluídos nos grupos de administração.

Para permitir a sondagem dos segmentos da nuvem, você deve ter os direitos correspondentes fornecidos com uma função do IAM ou conta de usuário IAM (no AWS), com um ID do Aplicativo e senha (no Azure), com um e-mail de cliente Google, ID de projeto Google e chave privada (no Google Cloud).

Você pode adicionar e excluir conexões, assim como definir o agendamento da sondagem, para cada segmento da nuvem.

Adicionando conexões para pesquisa de segmento de nuvem por meio do Kaspersky Security Center Cloud Console

Para adicionar uma conexão para a sondagem do segmento da nuvem para a lista de conexões disponíveis:

1. No menu principal, acesse **Descoberta e implementação → Descoberta → Nuvem**.
2. Na janela que se abre, clique em **Propriedades**.
3. Na janela **Configurações** que se abre, clique em **Adicionar**.

   A janela **Configurações de segmento da nuvem** se abre.

4. Especifique o nome do ambiente em nuvem para a conexão que será usada para a sondagem adicional do segmento da nuvem:

   - **Ambiente em nuvem**

     Selecione o ambiente em nuvem no qual você está implementando o Kaspersky Security Center Cloud Console: AWS, Azure ou Google Cloud.

     Caso planeje trabalhar com mais de um ambiente em nuvem, selecione um ambiente e execute o assistente novamente.

   - **Nome da conexão**

     Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

     Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

     Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

5. Insira suas credenciais para receber autorização no ambiente em nuvem que especificou.

   - Se você selecionou AWS, especifique o seguinte:

     - **ID da chave de acesso**

       A ID da chave de acesso IAM é uma sequência de caracteres alfanuméricos. Você recebeu a ID da chave quando você criou a conta de usuário IAM.

       O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização.

     - **Chave secreta**

       A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

       Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

       O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização.

       Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

   - Se você selecionou o Azure, especifique as seguintes configurações:

     - **ID do aplicativo Azure**

       Você criou este ID do aplicativo no portal do Azure.

       É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

     - **ID da assinatura do Azure**

Você criou a assinatura no portal do Azure.

- **Senha do aplicativo Azure**

  Você recebeu a senha quando criou o ID do aplicativo.

  Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

- **Nome da conta de armazenamento do Azure**

  Você criou o nome da conta de armazenamento do Azure para trabalhar com o Kaspersky Security Center Cloud Console.

- **Chave de acesso ao armazenamento do Azure**

  Você recebeu uma senha (chave) quando criou a conta de armazenamento Azure para trabalhar com o Kaspersky Security Center Cloud Console.

  A chave está disponível na seção "Visão geral da conta de armazenamento Azure", na subseção "Chaves".

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

Se você selecionou o Google Cloud, especifique as seguintes configurações:

- **Endereço de e-mail do cliente**

  O e-mail do cliente é o endereço usado para registrar o seu projeto no Google Cloud.

- **ID do projeto**

  O ID do projeto é o código recebido no ato do registro do seu projeto no Google Cloud.

- **Chave privada**

  A chave privada é a sequência de caracteres recebida como sua chave privada ao registrar o seu projeto no Google Cloud. Você pode copiar e colar esta sequência para evitar erros.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

6. Se quiser, clique em **Definir agendamento da sondagem** e altere as configurações padrão.

A conexão é salva nas configurações do aplicativo.

Após o novo segmento da nuvem ter sido amostrado pela primeira vez, um subgrupo que corresponde àquele segmento aparece no grupo de administração **Dispositivos gerenciados\Nuvem**.

Se você especificar as credenciais incorretas, nenhuma instância será encontrada durante a amostragem do segmento na nuvem e um novo subgrupo não aparecerá no grupo de administração **Dispositivos gerenciados\Cloud**.

Excluindo uma conexão para sondagem do segmento da nuvem

Se não for mais necessário sondar um segmento da nuvem específico, é possível excluir a conexão correspondente àquele segmento da lista de conexões disponíveis. Também é possível excluir uma conexão se, por exemplo, as permissões para sondar um segmento da nuvem tiverem sido transferidas para o outro usuário com credenciais diferentes.

Para excluir uma conexão:

1. No menu principal, acesse **Descoberta e implementação → Descoberta → Nuvem**.
2. Na janela que se abre, clique em **Propriedades**.
3. Na janela **Configurações** que se abre, clique no nome do segmento que deseja excluir.
4. Clique em **Excluir**.
5. Na janela que se abre, clique no botão **OK** para confirmar a sua seleção.

A conexão é excluída. Os dispositivos no segmento da nuvem correspondentes a essa conexão são excluídos automaticamente dos grupos de administração.

Configurando o agendamento da sondagem com o Kaspersky Security Center Cloud Console

A amostragem do segmento da nuvem é executada segundo um agendamento. Você pode definir a frequência de sondagem.

A frequência de sondagem é automaticamente definida como cinco minutos pelo Assistente de configuração de ambiente em nuvem. É possível alterar esse valor a qualquer momento e definir outro agendamento. Contudo, não é recomendado configurar a execução da sondagem mais frequentemente do que a cada 5 minutos porque isso pode levar a erros na operação da API.

Para configurar um agendamento da sondagem do segmento da nuvem:

1. No menu principal, acesse **Descoberta e implementação → Descoberta → Nuvem**.
2. Na janela que se abre, clique em **Propriedades**.
3. Na janela **Configurações** que se abre, clique no nome do segmento para o qual deseja configurar um agendamento de sondagem.

   A janela **Configurações de segmento da nuvem** se abre.
4. Na janela **Configurações de segmento da nuvem**, clique no botão **Definir agendamento da sondagem**.

   A janela **Agendamento** será aberta.

5. Na janela **Agendamento**, defina as seguintes configurações:

- **Início agendado**

  Opções de agendamento da sondagem:

  - A cada N dias

    A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

    Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

  - A cada N minutos

    A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

    Por padrão, a sondagem é executada a cada cinco minutos, iniciando na hora atual do sistema.

  - Por dias da semana

    A sondagem é executada regularmente, nos dias da semana e na hora especificados.

    Por padrão, a sondagem é executada todas as sextas-feiras às 18h.

  - Todos os meses em dias especificados das semanas selecionadas

    A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

    Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

- Intervalo de início (dias)

  Especifique o valor de N (para minutos ou dias).

- A partir das

  Especifique quando iniciar a primeira sondagem.

- Executar tarefas ignoradas

  Se o espaço de trabalho estiver indisponível no momento no qual a sondagem está agendada, o Kaspersky Security Center Cloud Console pode iniciar a sondagem imediatamente após ser ativado ou esperar até o próximo horário agendado.

  Se esta opção for ativada, o Kaspersky Security Center Cloud Console inicia a sondagem imediatamente após o espaço de trabalho estar disponível novamente.

  Se esta opção estiver desativada, o Kaspersky Security Center Cloud Console espera até a próxima sondagem agendada.

  Por padrão, esta opção está ativada.

6. Clique em **Salvar** para salvar as alterações.

O agendamento da sondagem para o segmento foi configurado e salvo.

Visualizando os resultados da sondagem de segmentos da nuvem com o Kaspersky Security Center Cloud Console

Você pode visualizar os resultados da amostragem de segmentos da nuvem, ou seja, visualizar a lista de dispositivos em nuvem gerenciados pelo Servidor de Administração.

Para visualizar os resultados da sondagem de segmentos da nuvem,

No menu principal, acesse **Descoberta e implementação → Descoberta → Nuvem**.

Os segmentos de nuvem disponíveis para pesquisa são exibidos.

Visualizando as propriedades dos dispositivos na nuvem usando o Kaspersky Security Center Cloud Console

É possível visualizar as propriedades de cada dispositivo na nuvem.

Para visualizar as propriedades de um dispositivo na nuvem:

1. No menu principal, vá para **Ativos (dispositivos) → Dispositivos gerenciados**.
2. Clique no nome do dispositivo cujas propriedades deseja visualizar.
   Uma janela de propriedades é exibida com a seção **Geral** selecionada.
3. Caso queira visualizar as propriedades específicas de dispositivos na nuvem, selecione a seção **Sistema** na janela de propriedades.
   As propriedades são exibidas dependendo da plataforma na nuvem do dispositivo.
   Para os dispositivos na AWS, as seguintes propriedades são exibidas:
   - **Dispositivo descoberto usando API** (valor: **AWS**)
   - **Região da nuvem**
   - **VPC da nuvem**
   - **Zona de disponibilidade da nuvem**
   - **Subrede da nuvem**
   - **Cloud Placement Group** (essa unidade será exibida apenas se a instância pertencer a um grupo de colocação; caso contrário, não será exibida)

   Para os dispositivos no Azure, as seguintes propriedades são exibidas:
   - **Dispositivo descoberto usando API** (valor: **Microsoft Azure**)

- **Região da nuvem**
- **Subrede da nuvem**

Para os dispositivos no Google Cloud, as seguintes propriedades são exibidas:

- **Dispositivo descoberto usando API** (valor: **Google Cloud**)
- **Região da nuvem**
- **VPC da nuvem**
- **Zona de disponibilidade da nuvem**
- **Subrede da nuvem**

Sincronização com a nuvem: configuração da regra móvel

Durante a operação do assistente de configuração de ambiente em nuvem, a regra Sincronizar com a nuvem é criada automaticamente. Esta regra permite migrar automaticamente os dispositivos detectados em cada sondagem, do grupo Dispositivos não atribuídos para o grupo Dispositivos gerenciados\Nuvem para tornar estes dispositivos disponíveis para o gerenciamento centralizado. Por padrão, a regra está ativa após ter sido criada. Você pode desativar, modificar ou forçar a regra a qualquer momento.

Para editar as propriedades da regra de Sincronizar com a nuvem e/ou forçar a regra:

1. No menu principal, acesse **Descoberta e implementação → Implementação e atribuição → Regras de migração**.

   Uma lista de regras de movimentação é aberta.

2. Na lista de regras de movimentação, selecione **Sincronizar com a nuvem**.

   A janela Propriedades da regra é aberta.

3. Se necessário, especifique as seguintes configurações na guia **Condições da regra**, na guia **Segmentos da nuvem**:

   - **O dispositivo está no segmento da nuvem**

     A regra só é aplicada aos dispositivos que estão no segmento da nuvem selecionado. Caso contrário, a regar se aplica a todos os dispositivos que tenham sido descobertos.

     Por padrão, esta opção está selecionada.

   - **Incluir objetos secundários**

     A regra se aplica a todos os dispositivos no segmento selecionado e em todas as subsecções da nuvem aninhadas. Caso contrário, a regra só é aplicada aos dispositivos que estão no segmento raiz.

     Por padrão, esta opção está selecionada.

   - **Migrar dispositivos de objetos aninhados para os subgrupos correspondentes**

Se essa opção é ativada, os dispositivos de objetos aninhados são automaticamente movidos aos subgrupos que correspondem à sua estrutura.

Se essa opção é desativada, os dispositivos de objetos aninhados são automaticamente movidos para a raiz do subgrupo Nuvem sem nenhuma ramificação adicional.

Por padrão, esta opção está ativada.

- **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente**

  Se esta opção estiver ativada, quando a estrutura do grupo **Dispositivos gerenciados\Nuvem** não tiver nenhum subgrupo que corresponda à seção que contém o dispositivo, o Kaspersky Security Center Cloud Console criará os subgrupos. Por exemplo, se uma nova sub-rede for descoberta durante a descoberta de dispositivos, um novo grupo com o mesmo nome será criado abaixo do grupo **Dispositivos gerenciados\Nuvem**.

  Se esta opção estiver desativada, o Kaspersky Security Center não Cloud Console não criará nenhum novo subgrupo. Por exemplo, se uma nova sub-rede for descoberta durante a sondagem da rede, um novo grupo com o mesmo nome não será criado sob o grupo **Dispositivos gerenciados\Nuvem**, e os dispositivos naquela sub-rede serão movidos para o grupo **Dispositivos gerenciados\Nuvem**.

  Por padrão, esta opção está ativada.

- **Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem**

  Se esta opção estiver ativada, o aplicativo excluirá do grupo Nuvem todos os subgrupos que não correspondem a nenhum dos objetos da nuvem existentes.

  Se esta opção estiver desativada, os subgrupos que não correspondem a nenhum dos objetos da nuvem existentes serão mantidos.

  Por padrão, esta opção está ativada.

Caso tenha ativado a opção **Sincronizar grupos de administração com estrutura de nuvem** ao usar o assistente de configuração de ambiente em nuvem, a regra **Sincronizar com a nuvem** é criada com as opções ativadas **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente** e **Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem**.

Se você não ativou a opção **Sincronizar grupos de administração com estrutura de nuvem**, a regra **Sincronizar com a nuvem** é criada com essas opções desativadas (desmarcadas). Se o seu trabalho com o Kaspersky Security Center Cloud Console precisar que a estrutura de subgrupos no subgrupo **Dispositivos gerenciados\Nuvem** coincida com a estrutura dos segmentos da nuvem, ative as opções **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente** e **Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem** nas propriedades da regra e, a seguir, force a regra.

4. Na lista suspensa **Dispositivo detectado usando a API**, selecione um dos seguintes valores:

   - **Não**. O dispositivo não pode ser detectado usando a API do AWS, Azure ou Google, ou seja, está fora do ambiente de nuvem ou está no ambiente de nuvem mas não pode ser detectado usando uma API por algum motivo.

   - **AWS**. O dispositivo é detectado usando a AWS API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do AWS.

   - **Azure**. O dispositivo é detectado usando a Azure API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do Azure.

   - **Google Cloud**. O dispositivo é detectado usando a Google API, ou seja, o dispositivo está definitivamente no ambiente de nuvem do Google.

- Nenhum valor. Este critério não pode ser aplicado.

5. Se necessário, defina outras propriedades da regra nas outras seções.

A regra de movimentação é configurada.

Instalação remota de aplicativos nas máquinas virtuais do Azure

Você deve ter uma licença válida para instalar aplicativos nas máquinas virtuais do Microsoft Azure.

O Kaspersky Security Center Cloud Console suporta as seguintes cenários:

- Um dispositivo cliente é detectado via API do Azure. A instalação é executada por meio de uma API. Usar a API do Azure significa que será possível instalar os seguintes aplicativos:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- Um dispositivo cliente é detectado por meio da Azure API. A instalação é realizada por meio de ponto de distribuição ou, se não houver um ponto de distribuição, manualmente, usando pacotes de instalação independente. Você pode instalar qualquer aplicativo compatível com o Kaspersky Security Center Cloud Console desta forma.

Para criar uma tarefa para instalação remota do aplicativo nas máquinas virtuais do Azure:

1. No menu principal, vá para **Ativos (dispositivos)** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.
3. Siga as instruções do assistente:
   a. Selecionar **Instalar o aplicativo remotamente** como o tipo de tarefa.
   b. Na página **Pacotes de instalação**, selecione **Instalação remota pela API do Microsoft Azure**.
   c. Ao selecionar a conta para acessar os dispositivos, use uma conta existente do Azure ou clique em **Adicionar** e insira as credenciais de sua conta do Azure:
      - Nome da conta do Azure

        Digite qualquer nome para as credenciais que você está especificando. Este nome será exibido na lista das contas a executarem a tarefa.
      - ID do aplicativo Azure

Você criou este ID do aplicativo no portal do Azure.

É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- **Senha do aplicativo Azure**

  Você recebeu a senha quando criou o ID do aplicativo.

  Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

d. Selecione os dispositivos relevantes no grupo **Dispositivos gerenciados\Nuvem**.

Após a conclusão do assistente, a tarefa para a instalação remota do aplicativo aparece na lista de tarefas.

Alteração do idioma da interface do Kaspersky Security Center Cloud Console

É possível selecionar o idioma da interface do Kaspersky Security Center Cloud Console.

Para alterar o idioma da interface:

1. No menu principal, vá para **Configurações** → **Idioma**.
2. Selecione um dos idiomas compatíveis com a localização.

Contatar o Suporte Técnico

Esta seção descreve como adquirir o suporte técnico e os termos com os quais está disponível.

Como obter suporte técnico

Se você não conseguir encontrar uma solução para seu problema na documentação do Kaspersky Security Center Cloud Console ou em nenhuma das fontes de informação sobre o aplicativo, contate o Suporte Técnico da Kaspersky. Os especialistas do Suporte Técnico responderão a todas as suas dúvidas sobre instalação e uso do Kaspersky Security Center Cloud Console.

A Kaspersky fornece suporte para o Kaspersky Security Center Cloud Console durante o ciclo de vida útil (consulte a página de ciclo de vida de suporte do produto). Antes de entrar em contato com o Serviço de Suporte Técnico, leia as regras de suporte.

Você pode entrar em contato com o Suporte Técnico de uma das seguintes maneiras:

- Visitando o site de Suporte Técnico
- Enviando uma solicitação para o Suporte Técnico a partir do portal Kaspersky CompanyAccount

Suporte técnico via Kaspersky CompanyAccount

O Kaspersky CompanyAccount é um portal para empresas que usam aplicativos Kaspersky. O portal Kaspersky CompanyAccount foi projetado para facilitar a interação entre os usuários e os especialistas da Kaspersky através de solicitações online. Você pode usar o Kaspersky CompanyAccount para monitorar o status e também armazenar um histórico das suas solicitações online.

Você pode registrar todos os funcionários da sua empresa com uma única conta no Kaspersky CompanyAccount. Uma única conta permite gerenciar centralmente solicitações de funcionários registrados enviadas para a Kaspersky, além de gerenciar os privilégios desses funcionários através do Kaspersky CompanyAccount.

O portal Kaspersky CompanyAccount está disponível nos seguintes idiomas:

- Inglês
- Espanhol
- Italiano
- Alemão
- Polonês
- Português
- Russo
- Francês

- Japonês

Para saber mais sobre o Kaspersky CompanyAccount, visite o site do Suporte Técnico.

Informações necessárias para os especialistas do Suporte Técnico da Kaspersky

Ao entrar em contato com os especialistas do Suporte Técnico da Kaspersky, podem ser solicitadas as seguintes informações:

- Informações gerais sobre o Kaspersky Security Center Cloud Console
- ID do espaço de trabalho
- Informações de licença
- Número de aplicativos instalados
- ID e status do locatário

É possível encontrar as informações na seção **Menu da sua conta** → **Suporte Técnico**. Copie e compartilhe essas informações para obter ajuda sobre o seu problema.

Fontes de informação sobre o aplicativo

Página do Kaspersky Security Center Cloud Console no site da Kaspersky

Na página do Kaspersky Security Center Cloud Console no site da Kaspersky, é possível exibir informações gerais sobre o aplicativo, suas funções e recursos.

Página do Kaspersky Security Center Cloud Console na Base de conhecimento

A *Base de Dados de Conhecimento* é uma seção do site de suporte técnico da Kaspersky.

Na página do Kaspersky Security Center Cloud Console na Base de conhecimento, é possível ler artigos que fornecem informações úteis, recomendações e respostas às perguntas frequentes sobre como comprar, instalar e utilizar o aplicativo.

Os artigos na Base de Dados de Conhecimento podem fornecer respostas às perguntas relacionadas ao Kaspersky Security Center Cloud Console como também a outros aplicativos da Kaspersky. Os artigos na Base de dados de conhecimento também podem conter novidades sobre o suporte técnico.

Discutir questões sobre os aplicativos Kaspersky com a comunidade

Se a sua pergunta não precisar de uma resposta imediata, você pode discuti-la com os especialistas da Kaspersky e outros usuários no nosso Fórum.

No Fórum, você pode visualizar tópicos de discussão, postar seus comentários e criar novos tópicos de discussão.

> É necessária uma conexão com a Internet para acessar os recursos do site.

Se você não puder encontrar uma solução para o problema, entre em contato com o Suporte técnico.

Problemas conhecidos

O Kaspersky Security Center Cloud Console tem algumas limitações que não são críticas para a operação do aplicativo:

- Quando a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* ou *Verificação de atualizações* é importada, a opção **Selecionar dispositivos aos quais a tarefa será atribuída** é ativada. Essas tarefas não podem ser atribuídas para uma seleção de dispositivos ou dispositivos específicos. Caso a tarefa *Baixar atualizações aos repositórios de pontos de distribuição* ou *Verificação de atualizações* seja atribuída aos dispositivos específicos, ela será importada incorretamente.

- Após a conclusão da tarefa de *Verificação de inventário* para um dispositivo Linux, uma tentativa de envio dos arquivos recebidos à Kaspersky para análise retorna um erro.

- Se você tentar fazer login no Kaspersky Security Center Cloud Console usando os Serviços de Federação do Active Directory (ADFS), mas as permissões necessárias estiverem ausentes, o Kaspersky Security Center Cloud Console retornará o erro "Credenciais inválidas", em vez de avisar o usuário sobre as permissões ausentes.

- A tarefa Gerenciar dispositivos não funciona corretamente para dispositivos que executam macOS.

- Na janela de diagnóstico remoto, clicar no botão **Baixar todo o arquivo** pode não resultar no download correto.

Glossário

Administrador do Kaspersky Security Center Cloud Console

A pessoa que gerencia a operação de aplicativos através do sistema Kaspersky Security Center Cloud Console de administração centralizada remota.

Agente de autenticação

Uma interface que permite concluir a autenticação para acessar discos rígidos criptografados e carregar o sistema operacional após a unidade de disco rígido do sistema ter sido criptografada.

Agente de Rede

Um componente do Kaspersky Security Center Cloud Console que permite a interação entre o Servidor de Administração e os aplicativos da Kaspersky instalados em um nó específico da rede (estação de trabalho ou servidor). Este componente é comum a todos os aplicativos da empresa para Microsoft® Windows®. Existem versões separadas do Agente de Rede para os aplicativos da Kaspersky desenvolvidos os SO Unix e macOS.

Aplicativo incompatível

Um aplicativo antivírus de um desenvolvedor de terceiros ou um aplicativo da Kaspersky que não aceita o gerenciamento através do Kaspersky Security Center Cloud Console.

Arquivo de chave

Um arquivo com o formato xxxxxxxx.key que torna possível usar um aplicativo da Kaspersky com uma licença de avaliação ou licença comercial.

Ataque de vírus

Uma série de tentativas deliberadas para infectar um dispositivo com um vírus.

Atualização disponível

Um conjunto de atualizações dos módulos de aplicativo da Kaspersky com atualizações críticas acumuladas por um determinado período.

Atualizar

O procedimento de substituição ou inclusão de novos arquivos (bancos de dados ou módulos de aplicativo), recebidos a partir dos servidores de atualização da Kaspersky.

Bancos de dados antivírus

Bancos de dados que contêm informações sobre ameaças à segurança do computador conhecidas da Kaspersky na data de publicação dos bancos de dados antivírus. As entradas em bancos de dados antivírus permitem a detecção de código malicioso em objetos verificados. Bancos de dados antivírus são criados pelos especialistas da Kaspersky e são atualizados a cada hora.

Chave ativa

Uma chave usada atualmente pelo aplicativo.

Chave de acesso AWS IAM

Uma combinação consistindo na ID da chave (que se parece com "AKIAIOSFODNN7EXAMPLE") e uma chave secreta (que se parece com "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Este par pertence ao Usuário do IAM e é usado para obter o acesso aos serviços AWS.

Chave de assinatura adicional

Uma chave que certifica que o usuário tem o direito de usar o aplicativo, mas que não está sendo usado no momento.

Configurações de Programa

As configurações do aplicativo que forem comuns para todos os tipos de tarefas e controlam a operação total do aplicativo, como: configurações de desempenho do aplicativo, configurações de relatórios e configurações de backup.

Configurações de tarefa

Configurações do aplicativo específicas para cada tipo de tarefa.

Console de Gerenciamento AWS

A interface da Web para visualizar e gerenciar recursos AWS. Console de Gerenciamento AWS está disponível na Web em https://aws.amazon.com/pt/.

Conta no Kaspersky Security Center Cloud Console

Uma conta de usuário necessária para configurar o Kaspersky Security Center Cloud Console, por exemplo, adicionando e removendo contas de usuário e configurando perfis de segurança (políticas de segurança). Esta conta permite usar o serviço My Kaspersky. Você cria esta conta quando começa a usar o Kaspersky Security Center Cloud Console.

Dispositivo de proteção UEFI

O dispositivo com o Kaspersky Anti-Virus para UEFI integrado no nível da BIOS. A proteção integrada assegura a segurança do dispositivo do momento do início do sistema, enquanto a proteção nos dispositivos sem software integrado somente começa a funcionar após o início do aplicativo de segurança.

Dispositivo gerenciado

Um computador com o Agente de Rede instalado ou um dispositivo móvel com um aplicativo de segurança Kaspersky instalado.

Domínio de difusão

A área lógica de uma rede na qual todos os nós podem intercambiar dados usando o canal de difusão no nível do OSI (Open Systems Interconnection Basic Reference Model).

Espaço de trabalho

Uma instância do Kaspersky Security Center Cloud Console criada para uma empresa específica. Quando um cliente cria um espaço de trabalho, a Kaspersky cria e configura a infraestrutura, e o Console de Administração baseado na nuvem é necessário para gerenciar os aplicativos de segurança instalados nos dispositivos da empresa.

Expert View do Kaspersky Next

Um aplicativo concebido para a execução centralizada de tarefas de administração e manutenção básicas na rede de uma organização. A Expert View do Kaspersky Next é hospedada e mantida pela Kaspersky. O aplicativo faz parte da solução em nuvem do Kaspersky Next. Nesta solução, você também pode usar o Pro View do Kaspersky Next.

Função do IAM

Conjunto de direitos para fazer solicitações aos serviços com base no AWS. As funções do IAM não são vinculadas à um usuário específico ou grupo; elas fornecem direitos de acesso sem as chaves de acesso AWS IAM. Você pode atribuir uma função do IAM aos usuários IAM, instâncias EC2, e aplicativos com base em AWS ou serviços.

Gateway de conexão

Um *gateway de conexão* é um Agente de Rede atuando em um modo especial. Um gateway de conexão aceita conexões de outros Agentes de Rede e os canaliza para o Servidor de Administração por meio de sua própria conexão com o Servidor. Ao contrário de um Agente de Rede comum, um gateway de conexão aguarda por conexões do Servidor de Administração, em vez de estabelecer conexões com o Servidor de Administração.

Gerenciamento centralizado de aplicativos

O gerenciamento remoto de aplicativo utilizando os serviços de administração fornecidos no Kaspersky Security Center Cloud Console.

Gerenciamento de identidades e acesso (IAM)

O serviço AWS que ativa o gerenciamento de acesso do usuário a outros serviços e recursos AWS.

Gerenciamento direto de aplicativos

Gerenciamento de aplicativos através de interface local.

Gravidade do evento

Propriedade de um evento encontrado durante a operação de um aplicativo da Kaspersky. Existem os seguintes níveis de gravidade:

- Evento crítico
- Falha funcional
- Advertência
- Informação

Eventos do mesmo tipo podem ter níveis de gravidade diferentes dependendo da situação na qual ocorreu o evento.

Grupo de administração

Um grupo de dispositivos agrupados por função e por aplicativos da Kaspersky instalados. Os dispositivos são agrupados como uma entidade única para a conveniência de gerenciamento. Um grupo pode incluir outros grupos. As políticas de grupo e tarefas de grupo podem ser criadas para cada aplicativo instalado no grupo.

HTTPS

Protocolo seguro para transferência de dados, usando criptografia, entre um navegador e um servidor da Web. HTTPS é usado para acessar informações restritas, como dados corporativos e financeiros.

Identificador do aplicativo

Um identificador para aplicativos de terceiros que pode ser usado para agrupar ou encontrar aplicativos. Uma tag destinada a aplicativos pode servir como uma condição em seleções de dispositivos.

Imagem de máquina da Amazon (AMI, Amazon Machine Image)

O modelo que contém a configuração do software necessária para executar a máquina virtual. Múltiplas instâncias podem ser criadas com base em uma única AMI.

Instalação forçada

O método para a instalação remota de aplicativos da Kaspersky que permite instalar o software em dispositivos cliente específicos. Para a conclusão com êxito da instalação forçada, a conta usada para essa tarefa deve ter direitos suficientes para a iniciar o aplicativo remotamente em dispositivos cliente. Esse método é recomendado para instalar aplicativos em dispositivos que executam os sistemas operacionais Microsoft Windows e que são compatíveis com essa funcionalidade.

Instalação local

Instalação de um aplicativo de segurança em um dispositivo em uma rede corporativa que supõe a inicialização de instalação manual do pacote de distribuição do aplicativo de segurança ou a inicialização manual de um pacote de instalação publicado que foi baixado previamente no dispositivo.

Instalação remota

Instalação de aplicativos da Kaspersky usando os serviços fornecidos pelo Kaspersky Security Center Cloud Console.

Instância Amazon EC2

Uma máquina virtual criada com base em uma imagem AMI usando Amazon Web Services.

Interface do Programa de Aplicativo AWS (AWS API)

A interface de programação do aplicativo da plataforma AWS que é usada pelo Kaspersky Security Center Cloud Console. Especificamente, as ferramentas de API da AWS são usadas para pesquisa de segmento da nuvem.

JavaScript

Uma linguagem de programação que expande o desempenho de páginas da Web. As páginas da Web criadas com JavaScript podem executar funções (por exemplo, alterar a visualização de elementos da interface ou abrir janelas adicionais) sem atualizar a página da Web com novos dados de um servidor da Web. Para visualizar as páginas criadas ao utilizar o JavaScript, ative o suporte do JavaScript na configuração do seu navegador.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network é uma solução que dá a usuários de dispositivos com aplicativos instalados da Kaspersky acesso a bancos de dados de reputação do Kaspersky Security Network e outros dados estatísticos sem enviar dados dos dispositivos ao Kaspersky Security Network. O Kaspersky Private Security Network foi projetado para clientes corporativos que não podem participar do Kaspersky Security Network por algum dos seguintes motivos:

- Os dispositivos não estão conectados à Internet.
- A transmissão de quaisquer dados fora do país ou da LAN corporativa é proibida pela lei ou por políticas de segurança corporativas.

Kaspersky Security Network (KSN)

Uma infraestrutura de serviços online que fornece o acesso aos banco de dados da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software constantemente atualizadas. O Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky quanto a ameaças, aprimora o desempenho de alguns componentes de proteção e reduz a probabilidade ocorrerem falsos positivos.

Limite de atividade de vírus

Número máximo permitido de eventos do tipo especificado dentro de um tempo limitado; quando excedido, é interpretado como um aumento da atividade de vírus e como uma ameaça de um ataque de vírus. Este recurso é importante durante períodos de ataques de vírus, já que permite aos administradores reagirem de modo oportuno às ameaças de ataques de vírus.

Nível de importância do patch

Atributo do patch. Há cinco níveis de importância para patches da Microsoft e para patches de terceiros:

- Crítico
- Alto
- Médio

- Baixo
- Desconhecido

O nível de importância de uma aplicação de patches de terceiros ou da aplicação de patches da Microsoft é determinado pelo nível de gravidade menos favorável entre as vulnerabilidades que os patches deveriam corrigir.

Operador do Kaspersky Security Center Cloud Console

Usuário que monitora o status e operação de um sistema de proteção gerenciado através do Kaspersky Security Center Cloud Console.

Pacote de instalação

Um conjunto de arquivos criados para a instalação remota de um aplicativo da Kaspersky usando o sistema de administração remota do Kaspersky Security Center Cloud Console. O pacote de instalação contém um intervalo de configurações necessárias para instalar o aplicativo e colocá-lo em funcionamento imediatamente após a instalação. As configurações correspondem aos padrões do aplicativo. O pacote de instalação é criado usando arquivos com as extensões .kpd e .kud incluídas no kit de distribuição do aplicativo.

Perfil da política

Um subconjunto nomeado de configurações de política. Este subconjunto é distribuído em dispositivos-alvo em conjunto com a política, complementando-a em uma condição específica denominada como condição de ativação do perfil.

Período da licença

Um período durante o qual você tem acesso aos recursos do aplicativo e possui direitos de usar serviços adicionais. Os serviços que você pode usar dependem do tipo de licença.

Plug-in da Web de gerenciamento

Um componente especial que é usado para a administração remota de softwares da Kaspersky por meio do Kaspersky Security Center Cloud Console. Um plugin de gerenciamento é uma interface entre o Kaspersky Security Center Cloud Console e um aplicativo da Kaspersky específico. Com um plug-in de gerenciamento, você pode configurar tarefas e políticas para o aplicativo.

Política

Uma política determina as configurações de um aplicativo e gerencia a capacidade de configurar esse aplicativo em computadores dentro de um grupo de administração. Uma política individual deve ser criada para cada aplicativo. Você pode criar várias políticas para aplicativos instalados nos computadores de cada grupo de administração, mas apenas uma política pode ser aplicada a cada aplicativo por vez em um grupo de administração.

Ponto de distribuição

Um computador que tenha o Agente de Rede instalado e que é usado para a distribuição de atualizações, sondagem de rede, instalação remota de aplicativos, obtenção de informações sobre os computadores em um grupo de administração e/ou domínio de difusão. O administrador seleciona os dispositivos apropriados e atribui a eles pontos de distribuição manualmente.

Proprietário do dispositivo

Proprietário do dispositivo é um usuário que pode ser contatado pelo administrador quando a necessidade surgir para executar determinadas operações em um dispositivo cliente.

Proteção antivírus da rede

Um conjunto de medidas técnicas e organizacionais que reduzem a probabilidade de penetração de vírus e spam em uma rede da organização e que previnem ataques na rede, phishing e outras ameaças. A segurança da rede aumenta quando você usa aplicativos e serviços de segurança e ao aplicar e aderir à política de segurança de dados corporativa.

Quarentena

Um repositório especial que armazena prováveis arquivos infectados com vírus e arquivos que não podem ser desinfectados no momento que são encontrados.

Repositório de eventos

Uma parte do banco de dados do Servidor de Administração dedicada ao armazenamento de informações sobre eventos que ocorrem no Kaspersky Security Center Cloud Console.

Restauração

A realocação do objeto original da Quarentena ou Backup para sua pasta original onde o objeto foi armazenado antes de entrar na Quarentena, antes de ter sido desinfetado ou excluído, ou realocação para uma pasta definida pelo usuário.

Servidor de Administração

Componente do Kaspersky Security Center Cloud Console que armazena centralmente informações sobre todos os aplicativos da Kaspersky instalados na rede empresarial. Pode também ser usado para gerenciar estes aplicativos.

Servidor de Administração Principal

Servidor de Administração principal é o Servidor de Administração que foi especificado durante a instalação do Agente de Rede. O Servidor de Administração principal pode ser usado em configurações de perfis de conexão do Agente de Rede.

Servidor de Administração virtual

Um componente do Kaspersky Security Center Cloud Console designado para gerenciamento do sistema de proteção de uma rede corporativa cliente.

O Servidor de Administração virtual é um caso particular de um Servidor de Administração secundário com as seguintes restrições em comparação com o Servidor de Administração físico:

- Servidores de Administração virtuais só funcionam como Servidores de Administração secundários.
- O Servidor de Administração virtual não é compatível com a criação de Servidores de Administração secundários (incluindo servidores virtuais).

Servidores de atualização da Kaspersky

Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.

SSL

Um protocolo de criptografia de dados usado na Internet e em redes locais. O protocolo Secure Sockets Layer (SSL) é usado em aplicativos da Web para criar uma conexão segura entre o cliente e o servidor.

Status de proteção

Status de proteção atual, que reflete o nível de segurança do computador.

Status de proteção da rede

O status de proteção atual, o qual define a segurança dos dispositivos na rede corporativa. O status de proteção da rede inclui fatores como os aplicativos de segurança instalados, o uso de chaves de licença e o número e os tipos de ameaças detectadas.

Tag de dispositivo

Um identificador de um dispositivo que pode ser usado para agrupar, descrever ou encontrar dispositivos.

Tarefa

Funções executadas pelo aplicativo da Kaspersky são implementadas como tarefas, tais como: Proteção do arquivo em tempo real, Verificação Completa do dispositivo, Atualização do banco de dados.

Tarefa de grupo

Uma tarefa definida para um grupo de administração e executada em todos os dispositivos cliente incluídos em tal grupo de administração.

Tarefa local

Uma tarefa definida e executada em um único computador cliente.

Tarefa para dispositivos específicos

Uma tarefa atribuída para um conjunto de dispositivos cliente a partir de grupos de administração arbitrários e executada nesses dispositivos.

Usuário do IAM

O usuário dos serviços AWS. Um usuário do IAM pode ter os direitos para executar a sondagem do segmento da nuvem.

Vulnerabilidade

Uma falha de um sistema operacional ou aplicativo que pode ser explorada por desenvolvedores de malware para invadir o sistema operacional ou aplicativo e violar sua integridade. Presença de um grande número de vulnerabilidades em um sistema operacional torna seu funcionamento não confiável, porque os vírus que invadiram o sistema operacional podem causar interrupções no próprio sistema operacional e em aplicativos instalados.

Zona desmilitarizada (DMZ)

A zona desmilitarizada é um segmento da rede local que contém servidores, os quais respondem a solicitações da Web global. Para assegurar a segurança da rede local de uma organização, o acesso à LAN a partir da zona desmilitarizada é protegido por um firewall.

Informação sobre código de terceiros

As informações sobre o código de terceiros estão contidas no arquivo legal_notices.txt.

O arquivo legal_notices.txt também está localizado na pasta de instalação do Agente de Rede para Windows e do Agente de Rede para Linux.

Para obter informações adicionais sobre códigos de terceiros utilizados nos espaços de trabalho, consulte a documentação do Kaspersky Endpoint Security Cloud.

Avisos de marca registrada

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

Adobe, Acrobat, Flash, PostScript, Reader, Shockwave são marcas comerciais registradas ou marcas comerciais da Adobe nos Estados Unidos e/ou outros países.

AMD64 é uma marca comercial ou marca registrada da Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS e AWS Marketplace são marcas comerciais da Amazon.com, Inc. ou de suas afiliadas.

Apache é uma marca registrada ou uma marca comercial da Apache Software Foundation.

Apple, App Store, AppleScript, FileVault, iPhone, iTunes, Mac, Mac OS, macOS, OS X, Safari e QuickTime são marcas comerciais da Apple Inc.

Arm é uma marca registrada da Arm Limited (ou de suas subsidiárias) nos Estados Unidos e/ou em outros lugares.

A palavra, marca e os logótipos Bluetooth são propriedade da Bluetooth SIG, Inc.

Ubuntu LTS são marcas comerciais registradas da Canonical Ltd.

Cisco, IOS e Cisco Jabber são marcas comerciais registradas ou marcas comerciais da Cisco Systems, Inc. e/ou de suas afiliadas nos Estados Unidos e em outros países específicos.

Citrix, XenServer são marcas comerciais da Citrix Systems, Inc. e/ou de uma ou mais de suas subsidiárias, e podem estar registradas no United States Patent and Trademark Office e em outros países.

Cloudflare, o logotipo da Cloudflare e Cloudflare Workers são marcas comerciais e/ou marcas registradas da Cloudflare, Inc. nos Estados Unidos e em outras jurisdições.

Corel e CorelDRAW são marcas comerciais ou marcas comerciais registradas da Corel Corporation e/ou de suas subsidiárias no Canadá, nos Estados Unidos e/ou em outros países.

Dropbox é uma marca registrada da Dropbox, Inc.

Radmin é marca registrada da Famatech.

Firebird é uma marca comercial registrada da Firebird Foundation.

Foxit é uma marca comercial registrada da Foxit Corporation.

FreeBSD é uma marca comercial registrada da The FreeBSD Foundation.

Google, Android, Chrome, Dalvik, Firebase, Google Chrome, Google Earth, Google Maps, Google Play e Google Public DNS são marcas comerciais da Google LLC.

EulerOS é uma marca comercial da Huawei Technologies Co., Ltd.

Intel e Core são marcas comerciais da Intel Corporation nos EUA e em outros países.

IBM, QRadar são marcas comerciais da International Business Machines Corporation registradas em muitas jurisdições em todo o mundo.

Node.js é uma marca registrada da Joyent, Inc.

Linux é uma marca comercial registrada da Linus Torvalds nos Estados Unidos e em outros locais.

Logitech é uma marca registrada ou marca comercial da Logitech nos Estados Unidos e/ou em outros países.

Microsoft, Active Directory, ActiveSync, ActiveX, BitLocker, Excel, Hyper-V, InfoPath, Internet Explorer, Microsoft Edge, MS-DOS, MultiPoint, Office 365, OneNote, Outlook, PowerPoint, PowerShell, Segoe, Skype, SQL Server, Tahoma, Visio, Win32, Windows, Windows Azure, Windows Media, Windows Mobile, Windows Phone, Windows Server, e Windows Vista são marcas comerciais do grupo de empresas da Microsoft.

CVE é uma marca comercial registrada da The MITRE Corporation.

Mozilla, Firefox e Thunderbird são marcas registradas da Mozilla Foundation nos EUA e em outros países.

Novell é uma marca comercial registrada da Novell Enterprises Inc. nos Estados Unidos e em outros países.

NetWare é uma marca comercial registrada da Novell Inc. nos Estados Unidos e em outros países.

Oracle, Java e JavaScript são marcas comerciais registradas da Oracle e/ou suas afiliadas.

Parallels, o logotipo da Parallels e Coherence são marcas comerciais ou marcas registradas da Parallels International GmbH.

Python é uma marca comercial ou marca registrada da Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS, Fedora são marcas comerciais ou marcas registradas da Red Hat, Inc. ou de suas subsidiárias nos Estados Unidos e em outros países.

BlackBerry é propriedade da Research In Motion Limited e está registrada nos Estados Unidos e poderá estar registrada ou com registro pendente em outros países.

Samsung é uma marca registrada da SAMSUNG nos Estados Unidos ou outros países.

Debian é uma marca registrada da Software in the Public Interest, Inc.

Splunk é uma marca comercial e marca comercial registrada da Splunk Inc. nos Estados Unidos e em outros países.

SUSE é uma marca comercial registrada da SUSE LLC nos Estados Unidos e em outros locais.

A marca comercial Symbian é propriedade da Symbian Foundation Ltd.

VMware, VMware vSphere e VMware Workstation são marcas comerciais registradas ou marcas comerciais da VMware, Inc. nos Estados Unidos e/ou em outras jurisdições.

UNIX é uma marca comercial registrada nos Estados Unidos e em outros países, licenciada exclusivamente pela X/Open Company Limited.