

kaspersky

Kaspersky Security Center 14 Linux

© 2023 AO Kaspersky Lab

Índice

[Ajuda do Kaspersky Security Center 14 Linux](#)

[O que há de novo](#)

[Sobre os certificados do Kaspersky Security Center Linux](#)

[Kit de distribuição](#)

[Requisitos de hardware e software](#)

[Sobre o Kaspersky Security Center 14 Web Console](#)

[Lista de aplicativos com suporte no Kaspersky](#)

[Comparativo do Kaspersky Security Center: baseado em Windows X baseado em Linux](#)

[Conceitos básicos](#)

[Servidor de Administração](#)

[Hierarquia de Servidores de Administração](#)

[Servidor de Administração virtual](#)

[Servidor Web](#)

[Agente de Rede](#)

[Grupos de administração](#)

[Dispositivo gerenciado](#)

[Dispositivo não atribuído](#)

[Estação de trabalho do administrador](#)

[Plug-in da Web de gerenciamento](#)

[Políticas](#)

[Perfis da política](#)

[Tarefas](#)

[Escopo da tarefa](#)

[Como as configurações do aplicativo local se relacionam com as políticas](#)

[Ponto de distribuição](#)

[Gateway de conexão](#)

[Licenciamento](#)

[Sobre o Contrato de Licença do Usuário Final](#)

[Sobre a licença](#)

[Sobre o certificado de licença](#)

[Sobre a chave de licença](#)

[Ler a Política de Privacidade](#)

[Opções de licença do Kaspersky Security Center](#)

[Sobre o arquivo de chave](#)

[Sobre a coleta de dados](#)

[Sobre a assinatura](#)

[Eventos do limite do licenciamento excedidos](#)

[Arquitetura](#)

[Diagrama de implementação do Servidor de Administração do Kaspersky Security Center e do Kaspersky Security Center 14 Web Console](#)

[Portas usadas pelo Kaspersky Security Center Linux](#)

[Portas usadas pelo Kaspersky Security Center 14 Web Console](#)

[Instalação](#)

[Cenário principal de implementação](#)

[Instalação de um sistema de gerenciamento de banco de dados](#)

[Configurando o servidor MariaDB x64 para trabalhar com o Kaspersky Security Center 14 Linux](#)

[Instalando o Kaspersky Security Center](#)

[Instalar o Kaspersky Security Center 14 Web Console](#)

[Parâmetros de instalação do Kaspersky Security Center 14 Web Console](#)

[Contas para trabalhar com o DBMS](#)

[Implementação do cluster de failover da Kaspersky](#)

[Cenário: implantando um cluster de failover Kaspersky](#)

[Sobre o cluster de failover da Kaspersky](#)

[Preparando um servidor de arquivos para um cluster de failover da Kaspersky](#)

[Preparando nós para um cluster de failover da Kaspersky](#)

[Instalando o Kaspersky Security Center nos nós do cluster de failover da Kaspersky](#)

[Iniciando e interrompendo nós de cluster manualmente](#)

[Certificados para trabalhar com o Kaspersky Security Center](#)

[Sobre os certificados do Kaspersky Security Center](#)

[Requisitos para certificados personalizados usados no Kaspersky Security Center](#)

[Reemissão do certificado do Kaspersky Security Center 14 Web Console](#)

[Substituir o certificado do Kaspersky Security Center 14 Web Console](#)

[Converter um certificado PFX para o formato PEM](#)

[Cenário: especificação do certificado personalizado do Servidor de Administração](#)

[Substituição do certificado do Servidor de Administração usando o utilitário klsetsrvcert](#)

[Conexão dos Agentes de Rede ao Servidor de Administração usando o utilitário klmover](#)

[Definir uma pasta compartilhada](#)

[Sobre atualizar o Kaspersky Security Center Linux](#)

[Atualizar o Kaspersky Security Center Linux usando o arquivo de instalação](#)

[Atualizar o Kaspersky Security Center Linux por meio de backup](#)

[Login no Kaspersky Security Center 14 Web Console e logout](#)

[Assistente de Início Rápido](#)

[Etapa 1. Especificando as configurações de conexão da Internet](#)

[Passo 2. Selecionando o método de ativação do aplicativo](#)

[Etapa 3. Criar uma configuração de proteção de rede básica](#)

[Etapa 4. Configurar as notificações por e-mail](#)

[Etapa 5. Fechar o Assistente de Início Rápido](#)

[Assistente de Implementação da Proteção](#)

[Iniciar o Assistente de Implementação da Proteção](#)

[Etapa 1. Seleção do pacote de instalação](#)

[Etapa 2. Seleção de um método de distribuição de arquivo de chave ou código de ativação](#)

[Etapa 3. Seleção de versão do Agente de Rede](#)

[Etapa 4. Seleção de dispositivos](#)

[Etapa 5. Especificação das configurações de tarefa de instalação remota](#)

[Etapa 6. Remoção de aplicativos incompatíveis antes de instalação](#)

[Etapa 7. Movimentação de dispositivos para dispositivos gerenciados](#)

[Etapa 8. Seleção de contas para acessar dispositivos](#)

[Etapa 9. Iniciando a instalação](#)

[Configurando o Servidor de Administração](#)

[Configuração da conexão do Kaspersky Security Center 14 Web Console ao Servidor de Administração](#)

[Configurando uma lista de permissão de endereços IP para fazer login no Kaspersky Security Center](#)

[Visualização do registro das conexões com o Servidor de Administração](#)

[Configuração do número máximo de eventos no repositório de eventos](#)

[Cópia backup e restauração dos dados do Servidor de Administração](#)

[Criando uma tarefa de backup de dados do Servidor de Administração](#)

[Utilitário de backup de dados e recuperação \(klbackup\)](#)

[Backup de dados e recuperação no modo interativo](#)

[Backup de dados e recuperação no modo não interativo](#)

[Mover o Servidor de Administração e um servidor de banco de dados para outro dispositivo](#)

[Criar um Servidor de Administração virtual](#)

[Uma hierarquia de Servidores de Administração](#)

[Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de Administração secundário](#)

[Visualizar a lista de Servidores de administração secundários](#)

[Ativando a proteção da conta contra modificações não autorizadas](#)

[Verificação em duas etapas](#)

[Cenário: configurando a verificação em duas etapas para todos os usuários](#)

[Sobre a verificação em duas etapas para uma conta](#)

[Ativando a verificação em duas etapas para sua própria conta](#)

[Ativando a verificação em duas etapas para todos os usuários](#)

[Desativando a verificação em duas etapas para uma conta de usuário](#)

[Desativando a verificação em duas etapas para todos os usuários](#)

[Excluindo contas da verificação em duas etapas](#)

[Gerando uma nova chave secreta](#)

[Editando o nome de um emissor do código de segurança](#)

[Alterar o número permitido de tentativas de entrada de senha](#)

[Alterando credenciais de DBMS](#)

[Excluir uma hierarquia de Servidores de Administração](#)

[Configurar interface](#)

[Localizar os dispositivos na rede](#)

[Cenário: Localizar dispositivos na rede](#)

[Sondagem do conjunto de IPs](#)

[Adição e modificação de um conjunto de IPs](#)

[Sondagem Zeroconf](#)

[Tags de dispositivo](#)

[Sobre as tags de dispositivo](#)

[Criando uma tag de dispositivo](#)

[Renomeando uma tag de dispositivo](#)

[Excluindo uma tag de dispositivo](#)

[Visualizando dispositivos aos quais uma tag está atribuída](#)

[Visualizando as tags atribuídas a um dispositivo](#)

[Identificação de um dispositivo manualmente](#)

[Removendo uma tag atribuído de um dispositivo](#)

[Visualização de regras para identificar dispositivos automaticamente](#)

[Edição de uma regra para identificar dispositivos automaticamente](#)

[Criação de uma regra para identificar dispositivos automaticamente](#)

[Execução de regras para identificar dispositivos automaticamente](#)

[Exclusão de uma regra para identificar dispositivos automaticamente](#)

[Tags de aplicativo](#)

[Sobre as tags de aplicativos](#)

[Criando uma tag de aplicativo](#)

[Renomeando uma tag de aplicativo](#)

[Atribuindo uma tag de aplicativos](#)

[Removendo tags atribuídas de um aplicativo](#)

[Excluir uma tag de aplicativos](#)

[Implementação dos aplicativos Kaspersky](#)

[Cenário: Verificando a implementação dos aplicativos Kaspersky](#)

[Adicionando plugins de gerenciamento para aplicativos Kaspersky](#)

[Criando pacotes de instalação a partir de um arquivo](#)

[Criar pacote de instalação autônomo](#)

[Visualizar a lista de pacotes de instalação independente](#)

[Instalação de aplicativos usando a tarefa de instalação remota](#)

[Instalar um aplicativo nos dispositivos específicos](#)

[Instalar um aplicativo usando as políticas de grupo do Active Directory](#)

[Instalando aplicativos nos Servidores de Administração secundários](#)

[Especificando configurações para instalação remota em dispositivos Unix](#)

[Substituição de aplicativos de segurança de terceiros](#)

[Remover aplicativos ou atualizações de software remotamente](#)

[Preparo de um dispositivo executando o SUSE Linux Enterprise Server 15 para instalação do agente de rede](#)

[Aplicativos Kaspersky: licenciamento e ativação](#)

[Licenciamento de aplicativos gerenciados](#)

[Adição de uma chave de licença ao repositório do Servidor de Administração](#)

[Implementando uma chave de licença para dispositivos cliente](#)

[Distribuição automática de uma chave de licença](#)

[Visualizando de informações sobre chaves de licença em uso](#)

[Excluindo uma chave de licença do repositório](#)

[Revogando o consentimento com um Contrato de Licença do Usuário Final](#)

[Renovando licenças para aplicativos da Kaspersky](#)

[Usando o Kaspersky Marketplace para escolher as soluções comerciais Kaspersky de sua preferência](#)

[Configurar a proteção da rede](#)

[Cenário: Configurar a proteção da rede](#)

[Sobre as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário](#)

[Configuração e propagação de políticas: abordagem centrada no dispositivo](#)

[Configuração e propagação de políticas: abordagem centrada no usuário](#)

[Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security](#)

[Configurações de política do Agente de Rede](#)

[Alterando a prioridade para as regras de migração de dispositivos](#)

[Tarefas](#)

[Sobre as tarefas](#)

[Sobre o escopo de tarefa](#)

[Criar uma tarefa](#)

[Como iniciar uma tarefa manualmente](#)

[Visualizando a lista de tarefas](#)

[Configurações de tarefa gerais](#)

[Iniciar o assistente para alterar a senha das tarefas](#)

[Etapa 1. Especificar as credenciais](#)

[Etapa 2. Selecionar uma ação a ser executada](#)

[Etapa 3. Visualizar os resultados](#)

[Visualização de resultados da execução de tarefas armazenados no Servidor de Administração](#)

[Gerenciamento de dispositivos cliente](#)

[Configurações de um dispositivo gerenciado](#)

- [Criação de grupos de administração](#)
- [Regras de migração de dispositivos](#)
 - [Criar regras para mover dispositivos](#)
 - [Copiar as regras para mover dispositivos](#)
 - [Condições para migrar uma regra de um dispositivo](#)
- [Adicionar dispositivos manualmente a um grupo de administração](#)
- [Migrando dispositivos manualmente para um grupo de administração](#)
- [Alterar o Servidor de Administração para dispositivos cliente](#)
- [Exibir e configurar as ações quando os dispositivos mostram inatividade](#)
- [Sobre os status do dispositivo](#)
- [Configurar a alternância dos status do dispositivo](#)
- [Políticas e perfis da política](#)
 - [Sobre as políticas e perfis de política](#)
 - [Sobre as configurações de bloqueio e bloqueadas](#)
 - [Herança de políticas e perfis de política](#)
 - [Hierarquia de políticas](#)
 - [Perfis de política em uma hierarquia de políticas](#)
 - [Como as configurações são implementadas em um dispositivo gerenciado](#)
- [Gerenciamento de políticas](#)
 - [Visualização da lista de políticas](#)
 - [Criação de uma política](#)
 - [Configurações da política gerais](#)
 - [Modificar uma política](#)
 - [Ativando o desativando uma opção de herança de política](#)
 - [Cópia de uma política](#)
 - [Mover uma política](#)
 - [Sincronização forçada](#)
 - [Visualizar o gráfico de status de distribuição da política](#)
 - [Exclusão de uma política](#)
- [Gerenciando perfis de política](#)
 - [Visualização dos perfis de uma política](#)
 - [Alteração de uma prioridade de perfil da política](#)
 - [Criar um perfil da política](#)
 - [Copiar um perfil de política](#)
 - [Criar uma regra de ativação do perfil da política](#)
 - [Excluir um perfil de política](#)
- [Usuários e funções dos usuários](#)
 - [Sobre as funções dos usuários](#)
 - [Configurar direitos de acesso aos recursos do aplicativo. Controle de acesso baseado em função](#)
 - [Direitos de acesso aos recursos do aplicativo](#)
 - [Funções de usuário predefinidas](#)
 - [Adicionar uma conta de usuário interno](#)
 - [Criar um grupo de usuários](#)
 - [Editar uma conta de usuário interno](#)
 - [Editar um grupo de usuários](#)
 - [Adicionar as contas de usuário em um grupo interno](#)
 - [Atribuir um usuário como um proprietário de dispositivo](#)
 - [Excluir um usuário ou um grupo de segurança](#)

[Criar uma função de usuário](#)

[Editar uma função de usuário](#)

[Editar o escopo de uma função de usuário](#)

[Excluir uma função de usuário](#)

[Associação de perfis da política a funções](#)

[Gerenciar revisões de objeto](#)

[Sobre as revisões do objeto](#)

[Reverter um objeto para uma revisão anterior](#)

[Exclusão de objetos](#)

[Usando o utilitário klscflag para abrir a porta 13291](#)

[Atualização dos bancos de dados e dos aplicativos da Kaspersky.](#)

[Cenário: Atualização regular dos bancos de dados e dos aplicativos Kaspersky.](#)

[Sobre atualização de bancos de dados, módulos de software e aplicativos da Kaspersky.](#)

[Criação da tarefa baixar atualizações no repositório do Servidor de Administração](#)

[Visualização de atualizações baixadas](#)

[Verificação das atualizações baixadas](#)

[Criar a tarefa para baixar as atualizações aos repositórios de pontos de distribuição](#)

[Adicionando fontes de atualizações para a tarefa Baixar atualizações no repositório do Servidor de Administração](#)

[Sobre usar os arquivos diff para atualizar bancos de dados e módulos do software Kaspersky.](#)

[Ativando o recurso de Baixar arquivos diff: cenário](#)

[Baixar atualizações por pontos de distribuição](#)

[Atualização de bancos de dados e módulos de software da Kaspersky em dispositivos offline](#)

[Ajuste de pontos de distribuição e gateways de conexão](#)

[Configuração padrão de pontos de distribuição: escritório único](#)

[Configuração padrão de pontos de distribuição: múltiplos pequenos escritórios remotos](#)

[Calcular o número e a configuração de pontos de distribuição](#)

[Atribuir os pontos de distribuição automaticamente](#)

[Atribuir os pontos de distribuição manualmente](#)

[Modificar a lista de pontos de distribuição para um grupo de administração](#)

[Ativando um servidor push](#)

[Gerenciar aplicativos de terceiros em dispositivos cliente](#)

[Cenário: Gerenciamento de Aplicativos](#)

[Sobre o Controle de Aplicativos](#)

[Obter e visualizar uma lista de arquivos executáveis instalados em dispositivos clientes](#)

[Criar uma categoria de aplicativos com conteúdo adicionado manualmente](#)

[Visualizando a lista de categorias de aplicativo](#)

[Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos](#)

[Monitoramento e relatórios](#)

[Cenário: Monitoramento e relatórios](#)

[Sobre os tipos do monitoramento e relatórios](#)

[Painel e widgets](#)

[Usar o painel](#)

[Adição de widgets ao painel](#)

[Ocultação de um widget do painel](#)

[Movimentação de um widget no painel](#)

[Alteração do tamanho ou da aparência do widget](#)

[Alteração das configurações do widget](#)

[Sobre o modo somente painel](#)

[Configurando o modo somente painel](#)

[Relatórios](#)

[Usar os relatórios](#)

[Criação de um modelo de relatório](#)

[Visualização e edição das propriedades do modelo de relatório](#)

[Exportar um relatório para um arquivo](#)

[Como gerar e visualizar um relatório](#)

[Criação de uma tarefa de entrega de relatório](#)

[Excluir os modelos de relatório](#)

[Eventos e seleções de eventos](#)

[Usar as seleções de eventos](#)

[Criar uma seleção de eventos](#)

[Editar uma seleção de eventos](#)

[Visualizando uma lista de uma seleção de evento](#)

[Visualização dos detalhes de um evento](#)

[Exportar eventos para um arquivo](#)

[Visualização de um histórico de eventos a partir de um evento](#)

[Excluir os eventos](#)

[Excluir as seleções de eventos](#)

[Configuração do termo de armazenamento de um evento](#)

[Tipos de eventos](#)

[Estrutura de dados da descrição do tipo de evento](#)

[Eventos do Servidor de Administração](#)

[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](#)

[Eventos do Agente de Rede](#)

[Eventos de aviso do Agente de Rede](#)

[Eventos informativos do Agente de Rede](#)

[Bloqueio de eventos frequentes](#)

[Sobre o bloqueio de eventos frequentes](#)

[Gerenciando o bloqueio de eventos frequentes](#)

[Removendo o bloqueio de eventos frequentes](#)

[Processamento e armazenamento do evento no Servidor de Administração](#)

[Notificações e status do dispositivo](#)

[Usar as notificações](#)

[Visualização de notificações na tela](#)

[Sobre os status do dispositivo](#)

[Configurar a alternância dos status do dispositivo](#)

[Configurar a entrega de notificações](#)

[Testar as notificações](#)

[Notificações de evento exibidas executando um arquivo executável](#)

[Novidades da Kaspersky](#)

[Sobre as Novidades Kaspersky](#)

[Especificando configurações para receber as Novidades Kaspersky](#)

[Desativando o recebimento de Novidades Kaspersky](#)

[Exportação de eventos para os sistemas SIEM](#)

[Cenário: configurando a exportação de eventos para um sistema SIEM](#)

[Antes de iniciar](#)

[Sobre eventos no Kaspersky Security Center Linux](#)

[Sobre a exportação de evento](#)

[Sobre a configuração de exportação de eventos em um sistema SIEM](#)

[Marcando eventos para exportação para sistemas SIEM em formato Syslog](#)

[Sobre a marcação de eventos para exportação para o sistema SIEM no formato Syslog](#)

[Marcando eventos de um aplicativo da Kaspersky para exportação em formato Syslog](#)

[Marcando eventos gerais para exportação no formato Syslog](#)

[Sobre a exportação de eventos usando o formato Syslog](#)

[Configurando o Kaspersky Security Center Linux para exportação de eventos para o sistema SIEM](#)

[Exportando eventos diretamente do banco de dados](#)

[Criar uma consulta SQL usando o utilitário klsq2](#)

[Exemplo de uma consulta SQL no utilitário klsq2](#)

[Exibir o nome de banco de dados do Kaspersky Security Center Linux](#)

[Exibir os resultados da exportação](#)

[Seleções de dispositivos](#)

[Criar uma seleção de dispositivos](#)

[Configurar uma seleção de dispositivos](#)

[Guia de referência de API](#)

[Integração entre o Kaspersky Security Center Web Console e outras soluções](#)

[Configurar o acesso ao Console da Web KATA / KEDR](#)

[Estabelecendo uma conexão em segundo plano](#)

[Contatar o Suporte Técnico](#)

[Como obter suporte técnico](#)

[Obter suporte técnico por telefone](#)

[Suporte Técnico via Kaspersky CompanyAccount](#)

[Fontes de informação sobre o aplicativo](#)

[Problemas conhecidos](#)

[Glossário](#)

[Administrador cliente](#)

[Administrador do Kaspersky Security Center](#)

[Administrador do provedor de serviço](#)

[Agente de autenticação](#)

[Agente de Rede](#)

[Aplicativo incompatível](#)

[Arquivo de chave](#)

[Atualização disponível](#)

[Atualizar](#)

[Backup de dados do Servidor de Administração](#)

[Bancos de dados antivírus](#)

[Certificado compartilhado](#)

[Certificado do Servidor de Administração](#)

[Chave ativa](#)

[Chave de assinatura adicional](#)

[Configurações de Programa](#)

[Configurações de tarefa](#)

[Console de Administração](#)

[Direitos de administrador](#)

[Dispositivos gerenciados](#)

[Domínio de difusão](#)

[Estação de trabalho do administrador](#)

[Gateway de conexão](#)

[Gerenciamento centralizado de aplicativos](#)

[Gerenciamento direto de aplicativos](#)

[Gravidade do evento](#)

[Grupo de administração](#)

[Grupo de aplicativos licenciados](#)

[Grupo de funções](#)

[HTTPS](#)

[Instalação local](#)

[Instalação manual](#)

[Instalação remota](#)

[JavaScript](#)

[Kaspersky Private Security Network \(KSN Privada\)](#)

[Loja de aplicativos](#)

[Operador do Kaspersky Security Center](#)

[Pacote de instalação](#)

[Pasta de backup](#)

[Perfil](#)

[Perfil de configuração](#)

[Perfil de provisionamento](#)

[Período da licença](#)

[Política](#)

[Ponto de distribuição](#)

[Proprietário do dispositivo](#)

[Proteção antivírus da rede](#)

[Provedor de serviço de proteção antivírus](#)

[Repositório de eventos](#)

[Restauração](#)

[Restauração dos dados do Servidor de Administração](#)

[Servidor de Administração](#)

[Servidor de Administração cliente \(Dispositivo cliente\)](#)

[Servidor de Administração Principal](#)

[Servidor de Administração virtual](#)

[Servidor Web do Kaspersky Security Center](#)

[Servidores de atualização da Kaspersky](#)

[SSL](#)

[Status de proteção](#)

[Status de proteção da rede](#)

[Tarefa](#)

[Tarefa de grupo](#)

[Tarefa local](#)

[Tarefa para dispositivos específicos](#)

[Usuários internos](#)










[Validador de Integridade do Sistema do Kaspersky Security Center \(SHV\)](#)

[Zona desmilitarizada.\(DMZ\).](#)

[Informação sobre código de terceiros](#)

[Avisos de marca registrada](#)

Ajuda do Kaspersky Security Center 14 Linux

	<u>O que há de novo</u> Descubra o que há de novo na versão mais recente do aplicativo.		<u>Aplicativos da Kaspersky. Licenciamento e ativação</u> Ative os aplicativos Kaspersky em algumas etapas.
	<u>Requisitos de hardware e software</u> Verifique quais sistemas operacionais e versões de aplicativo são compatíveis		<u>Configurar a proteção da rede</u> Gerencie a segurança da organização.
	<u>Instalação</u> Servidor de Administração e Kaspersky Security Center 14 Web Console.		<u>Aplicativos da Kaspersky. Atualização dos bancos de dados e módulos de software</u> Mantenha a confiabilidade do sistema de proteção.
	<u>Localizar os dispositivos na rede</u> Detecte os dispositivos existentes e os novos na rede da sua organização.		<u>Monitoramento e relatórios</u> Visualize sua infraestrutura, status de proteção e estatísticas.
	<u>Aplicativos da Kaspersky. Implementação centralizada</u> Implementar aplicativos Kaspersky.		<u>Ajustar de pontos de distribuição e/ou gateways de conexão</u> Configurar os pontos de distribuição.

O que há de novo

Kaspersky Security Center 14 Linux

O Kaspersky Security Center 14 Linux inclui vários novos recursos e aprimoramentos:

- Além da tarefa [Baixar atualizações no repositório do Servidor de Administração](#), os bancos de dados antivírus para aplicativos de segurança da Kaspersky agora podem ser baixados por meio da tarefa [Baixar atualizações para os repositórios de pontos de distribuição](#).
- Bancos de dados de antivírus e módulos de aplicativos nos dispositivos gerenciados podem ser propagados e atualizados por meio do Servidor de Administração ou dos pontos de distribuição. É possível [escolher um esquema de atualização](#) ideal para sua organização, reduzir a carga no Servidor de Administração e otimizar o tráfego de dados na rede corporativa.
- O Kaspersky Security Center baixa dos servidores de atualização da Kaspersky apenas as atualizações solicitadas pelos aplicativos de segurança da Kaspersky. Isso reduz o tamanho dos dados baixados.
- Agora é possível usar o [recurso de arquivos diff](#) para baixar bancos de dados de antivírus e módulos de software. 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 poupa tráfego na rede da empresa porque os arquivos diff ocupam menos espaço do que arquivos completos de bancos de dados e módulos de software.
- A tarefa [Verificação de atualizações](#) foi adicionada. Ao usar essa tarefa, é possível verificar automaticamente as atualizações baixadas quanto à operacionalidade e erros antes de instalar as atualizações nos dispositivos gerenciados.

Sobre os certificados do Kaspersky Security Center Linux

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

O Kaspersky Security Center Linux (também conhecido como Kaspersky Security Center) foi desenvolvido para implementar e gerenciar a proteção de dispositivos Linux® utilizando o servidor de administração baseado em Linux para atender aos requisitos de ambientes exclusivamente Linux.

O Kaspersky Security Center Linux permite instalar aplicativos de segurança da Kaspersky em dispositivos em uma rede corporativa, executar remotamente as tarefas de verificação e atualização, além de gerenciar as políticas de segurança dos aplicativos gerenciados. É possível utilizar um painel detalhado que fornece uma visão instantânea do status de dispositivos corporativos, relatórios detalhados e configurações granulares nas políticas de proteção.

Comparado ao Kaspersky Security Center, que possui o Servidor de Administração baseado no Windows®, o Kaspersky Security Center Linux possui um [conjunto de recursos diferente](#).

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

Com o uso do Kaspersky Security Center, você pode fazer o seguinte:

- Crie uma hierarquia de Servidores de Administração para gerenciar a rede corporativa, assim como redes em escritórios remotos e organizações cliente.
A organização cliente é uma organização, cuja proteção antivírus é garantida pelo provedor de serviços.
- Crie uma hierarquia de grupos de administração para gerenciar uma seleção de dispositivos cliente como um todo.
- Gerenciar um sistema de proteção antivírus criado com base nos aplicativos Kaspersky.
- Execute a instalação remota de aplicativos pela Kaspersky e outros fornecedores de software.
- Realizar implementações centralizadas de chaves de licença para aplicativos Kaspersky em dispositivos cliente, monitorar seu uso e renovar licenças.
- Receber estatísticas e relatórios sobre a operação dos aplicativos e dispositivos.
- Receber notificações sobre eventos críticos durante a operação dos aplicativos Kaspersky.
- Realizar inventário de hardware conectado à rede corporativa.
- Gerencie centralizadamente os arquivos colocados em Quarentena ou em Backup pelos aplicativos de segurança, assim como gerencie os arquivos para os quais o processamento pelos aplicativos antivírus foi adiado.

Kit de distribuição

É possível comprar o aplicativo em lojas online da Kaspersky (por exemplo, em <https://www.kaspersky.com>) ou por meio de empresas parceiras.

Se você comprar o Kaspersky Security Center Linux em uma loja online, copie o aplicativo diretamente do site da loja. As informações necessárias para ativação do aplicativo são enviadas a você por e-mail após o pagamento.

Requisitos de hardware e software

Servidor de Administração

Requisitos mínimos de hardware:

- CPU com frequência operacional de 1 GHz ou superior. Para um sistema operacional de 64 bits, a frequência mínima de CPU é de 1.4 GHz.
- RAM: 4 GB.
- Espaço disponível em disco: 10 GB.

Os seguintes sistemas operacionais são compatíveis:

- Debian GNU / Linux 11.x (Bullseye) 32 bits / 64 bits
- Debian GNU/Linux 10.x (Buster) 32-bit/64-bit
- Debian GNU/Linux 9.x (Stretch) 32 bits/64 bits
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64 bits
- CentOS 7.x 64 bits
- Red Hat Enterprise Linux Server 8.x 64 bits
- Red Hat Enterprise Linux Server 7.x 64 bits
- SUSE Linux Enterprise Server 12 (todos Service Packs) 64 bits
- SUSE Linux Enterprise Server 15 (todos Service Packs) 64 bits
- Astra Linux Special Edition 1.7 (incluindo o [modo de ambiente de software fechado](#) e o modo obrigatório) de 64 bits
- Astra Linux Special Edition 1.6 (incluindo o modo de ambiente de software fechado e o modo obrigatório) de 64 bits
- Astra Linux Common Edition 2.12 64 bits
- Alt Server 10 64 bits
- Alt Server 9.2 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

- Oracle Linux 7 64 bits
- Oracle Linux 8 64 bits
- RED OS 7.3 Server 64 bits
- RED OS 7.3 Certified Edition 64 bits

As seguintes plataformas para virtualização são suportadas:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 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
- Máquina virtual baseada em kernel. Suporta os seguintes sistemas operacionais:
 - Alt 8 SP Server (LKNV.11100-01) 64 bits
 - Alt Server 10 64 bits
 - Astra Linux Special Edition 1.7 (incluindo o [modo de ambiente de software fechado](#) e o modo obrigatório) de 64 bits
 - Debian GNU / Linux 11.x (Bullseye) 32 bits / 64 bits
 - Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits
 - RED OS 7.3 Server 64 bits
 - RED OS 7.3 Certified Edition 64 bits

Os seguintes servidores de banco de dados são compatíveis (podem ser instalados em um dispositivo diferente):

- MySQL 5.7 Community 32 bits/64 bits
- MySQL 8.0 32 bits / 64 bits
- MariaDB 10.5.x 32 bits/64 bits

- MariaDB 10.4.x 32 bits/64 bits
- MariaDB 10.3.22 e superior 32 bits/64 bits
- MariaDB Server 10.3 32 bits/64 bits com mecanismo de armazenamento InnoDB
- MariaDB 10.1.30 e superior 32 bits/64 bits

Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console Server

Requisitos mínimos de hardware:

- CPU: 4 núcleos, frequência operacional de 2,5 GHz.
- RAM: 8 GB.
- Espaço disponível em disco: 40 GB.

Um dos seguintes sistemas operacionais (somente versões de 64 bits):

- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 9.x (Stretch)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- CentOS 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 12 (todos os Service Packs)
- SUSE Linux Enterprise Server 15 (todos os Service Packs)
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 bits
- Astra Linux Special Edition 1.7 (incluindo o [modo de ambiente de software fechado](#) e o modo obrigatório)
- Astra Linux Special Edition 1.6 (incluindo o modo de ambiente de software fechado e o modo obrigatório)
- Astra Linux Common Edition 2.12
- Alt Server 10
- Alt Server 9.2

- Alt 8 SP Server (LKNV.11100-01)
- Alt 8 SP Server (LKNV.11100-02)
- Alt 8 SP Server (LKNV.11100-03)
- Oracle Linux 8
- Oracle Linux 7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition

Entre as plataformas de virtualização, a máquina virtual baseada em kernel é compatível com os seguintes sistemas operacionais:

- Alt 8 SP Server (LKNV.11100-01) 64 bits
- Alt Server 10 64 bits
- Astra Linux Special Edition 1.7 (incluindo o [modo de ambiente de software fechado](#) e o modo obrigatório) de 64 bits
- Debian GNU / Linux 11.x (Bullseye) 32 bits / 64 bits
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits
- RED OS 7.3 Server 64 bits
- RED OS 7.3 Certified Edition 64 bits

Dispositivos cliente

Em um dispositivo cliente, o uso do Kaspersky Security Center 14 Web Console requer apenas um navegador.

Os requisitos de hardware e software para o dispositivo são idênticos aos requisitos do navegador utilizado com o Kaspersky Security Center 14 Web Console.

Navegadores:

- Mozilla Firefox Extended Support Release 91.8.0 ou superior (91.8.0 lançado em 5 de abril de 2022)
- Mozilla Firefox Versão 99.0 ou superior (99.0 lançada em 5 de abril de 2022)
- Google Chrome 100.0.4896.88 ou superior (compilação oficial)
- Microsoft Edge 100 ou superior
- Safari 15 no macOS

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.

Requisito de software para dispositivos baseados em Linux: o intérprete de linguagem Perl versão 5.10 ou superior deve estar instalado.

Os seguintes sistemas operacionais são compatíveis:

- Debian GNU / Linux 11.x (Bullseye) 32 bits / 64 bits
- Debian GNU/Linux 10.x (Buster) 32-bit/64-bit
- Debian GNU/Linux 9.x (Stretch) 32 bits/64 bits
- Ubuntu Server 20.04 LTS (Focal Fossa) 32 bits/64 bits
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 bits
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32 bits/64 bits
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bit/64-bit
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 bits/64 bits
- CentOS 8.x 64 bits
- CentOS 7.x 64 bits
- CentOS 7.x ARM 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 Service Packs) 64 bits
- SUSE Linux Enterprise Desktop 15 (todos os Service Packs) 64 bits
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 bits
- openSUSE 15 64 bits
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64 bits

- Astra Linux Special Edition 1.7 (incluindo o [modo de ambiente de software fechado](#) e o modo obrigatório) de 64 bits
- Astra Linux Special Edition 1.6 (incluindo o modo de ambiente de software fechado e o modo obrigatório) de 64 bits
- Astra Linux Common Edition 2.12 64 bits
- Astra Linux Special Edition 4.7 ARM
- 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
- Mageia 4 32 bits
- Oracle Linux 7 64 bits
- Oracle Linux 8 64 bits
- Linux Mint 19.x 32 bits
- Linux Mint 20.x 64 bits
- AlterOS 7.5 e versões posteriores 64 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 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
- Lotos (Linux Core versão 4.19.50, DE: MATE) 64 bits

As seguintes plataformas para virtualização são suportadas:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 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
- Máquina virtual baseada em kernel. Suporta os seguintes sistemas operacionais:
 - Alt 8 SP Server (LKNV.11100-01) 64 bits
 - Alt Server 10 64 bits
 - Astra Linux Special Edition 1.7 (incluindo o [modo de ambiente de software fechado](#) e o modo obrigatório) de 64 bits
 - Debian GNU / Linux 11.x (Bullseye) 32 bits / 64 bits
 - Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits
 - RED OS 7.3 64 bits
 - RED OS 7.3 Server 64 bits
 - RED OS 7.3 Certified Edition 64 bits

Recomendamos a instalação da mesma versão do Agente de Rede para Linux que o Kaspersky Security Center Linux.

Sobre o Kaspersky Security Center 14 Web Console

O Kaspersky Security Center 14 Web Console é um aplicativo concebido para gerenciar o status do sistema de segurança da rede protegida por aplicativos Kaspersky.

Usando o aplicativo, você pode:

- Gerenciar o status do sistema de segurança da organização.
- Instalar aplicativos Kaspersky em dispositivos em sua rede e gerenciar aplicativos instalados.
- Gerencie as políticas criadas para seus dispositivos na sua rede.
- Gerenciar contas de usuário.
- Gerenciar tarefas para aplicativos instalados em dispositivos na sua rede.
- Exibir relatórios sobre o status do sistema de segurança.
- Gerenciar a entrega de relatórios aos administradores do sistema e outros especialistas de TI.

Kaspersky Security Center 14 Web Console fornece uma interface da Web que assegura 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. O Servidor de Administração se conecta com os dispositivos em sua rede através de canais protegidos pelo protocolo Secure Socket Layer (SSL). Quando você se conecta ao Kaspersky Security Center 14 Web Console usando seu navegador, o navegador estabelece uma conexão com o servidor do Kaspersky Security Center 14 Web Console.

Você opera o Kaspersky Security Center 14 Web Console da seguinte maneira:

1. Use um navegador para se conectar ao Kaspersky Security Center 14 Web Console, onde a interface do portal da Web é exibida.
2. Use controles do portal da Web para escolher o comando que você deseja executar. O Kaspersky Security Center 14 Web Console executa as seguintes operações:
 - Se você tiver escolhido um comando usado para a recepção de informações (por exemplo, para visualizar uma lista de dispositivos), o Kaspersky Security Center 14 Web Console gera uma solicitação de informação ao Servidor de Administração, recebe os dados necessários e os envia para o navegador em um formato de fácil visualização.
 - Se você tiver escolhido um comando usado para o gerenciamento (por exemplo, instalação remota de um aplicativo), o Kaspersky Security Center 14 Web Console recebe o comando do navegador e o envia para o Servidor de Administração. A seguir, o aplicativo recebe o resultado do Servidor de Administração e o envia para o navegador em um formato de fácil visualização.

O Kaspersky Security Center 14 Web Console é um aplicativo disponível em vários idiomas. Você pode alterar o idioma da interface a qualquer momento, sem necessidade de reabrir o aplicativo. Ao instalar o Kaspersky Security Center 14 Web Console com o Kaspersky Security Center 14 Web Console, a solução usa o mesmo idioma de interface que o arquivo de instalação. Quando você instala apenas o Kaspersky Security Center 14 Web Console, o aplicativo usa o mesmo idioma da interface do seu sistema operacional. Se o Kaspersky Security Center 14 Web Console não for compatível com o idioma do arquivo de instalação ou do sistema operacional, o inglês será definido por padrão.

Lista de aplicativos com suporte no Kaspersky

O Kaspersky Security Center Linux oferece suporte à implantação e gerenciamento centralizados do Kaspersky Endpoint Security for Linux. Este aplicativo permite proteger estações de trabalho e servidores de arquivos. Consulte a [Página da Web do ciclo de vida do suporte ao produto](#) para obter as versões dos aplicativos.

Comparativo do Kaspersky Security Center: baseado em Windows X baseado em Linux

A Kaspersky fornece o Kaspersky Security Center como uma solução local para duas plataformas: Windows e Linux. Na solução baseada em Windows, você instala o Servidor de Administração em um dispositivo Windows e a solução baseada em Linux tem a versão do Servidor de Administração projetada para ser instalada em um dispositivo Linux.

A tabela abaixo permite comparar os principais recursos do Kaspersky Security Center como uma solução baseada no Windows e como uma solução baseada no Linux.

Comparativo de recursos do Kaspersky Security Center funcionando como uma solução baseada em Windows e uma solução baseada em Linux

Recurso ou propriedade	Kaspersky Security Center	
	Solução baseada em Windows	Solução baseada em Linux
Localização do Servidor de Administração	No local	No local
Localização do sistema de gerenciamento de banco de dados (DBMS)	No local	No local
Sistema operacional para instalar o Servidor de Administração	Windows	Linux
Tipo de console de administração	Local e baseado na web	Baseado na web
Sistema operacional para instalar o Console de Administração baseado na web no	Windows ou no Linux	Windows ou no Linux
Hierarquia de Servidores de Administração	✓	✓
Hierarquia do grupo de administração	✓	✓
Sondagem da rede	✓	✓ (apenas por intervalos de IP)
Número máximo de dispositivos gerenciados	100000	20000
Proteção de dispositivos gerenciados Windows, macOS e Linux	✓	— (proteção apenas para dispositivos Linux)
Proteção de dispositivos móveis	✓	—
Proteção de máquinas virtuais	✓	—
Proteção da infraestrutura de nuvem pública	✓	—
Gerenciamento de segurança centrada no dispositivo	✓	✓
Gerenciamento de segurança centrada no usuário	✓	✓
Políticas do aplicativo	✓	✓
Tarefas para aplicativos da Kaspersky	✓	✓
Kaspersky Security Network	✓	—

Proxy da KSN	✓	—
Kaspersky Private Security Network	✓	—
Implementação centralizada de chaves de licença para aplicativos da Kaspersky	✓	✓
Suporte para Servidores de administração virtuais	✓	✓
Instalar atualizações de softwares de terceiros e corrigir vulnerabilidades de softwares de terceiros	✓	— (usando apenas uma tarefa de instalação remota)
Notificações sobre eventos ocorridos em dispositivos gerenciados	✓	✓
Criação e gerenciamento de contas de usuário	✓	✓
Monitoramento do status de políticas e tarefas	✓	✓
Implementação do cluster de failover da Kaspersky	✓	✓

Conceitos básicos

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

Servidor de Administração

Os componentes do Kaspersky Security Center permitem o gerenciamento remoto dos aplicativos Kaspersky instalados em dispositivos cliente.

Os dispositivos com o componente do Servidor de Administração instalado serão referidos como *Servidores de Administração* (aqui referidos como *Servidores*). Os Servidores de Administração devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

O Servidor de Administração é instalado em um dispositivo como um serviço com o seguinte conjunto de atributos:

- Com o nome "Servidor de Administração do Kaspersky Security Center"
- Configurado para iniciar automaticamente ao inicializar o sistema operacional
- Com a conta **LocalSystem** ou a conta do usuário selecionada durante a instalação do Servidor de Administração

O Servidor de Administração realiza as seguintes funções:

- Armazenamento da estrutura dos grupos de administração
- Armazenamento de informações sobre a configuração de dispositivos cliente
- Organização dos repositórios para pacotes de distribuição de aplicativos
- Instalação remota de aplicativos para dispositivos cliente e remoção de aplicativos
- Atualização de bancos de dados de aplicativos e módulos de software dos aplicativos Kaspersky
- Gerenciamento de políticas e tarefas nos dispositivos cliente
- Armazenamento de informações sobre eventos que ocorreram em dispositivos cliente
- Geração de relatórios na operação dos aplicativos Kaspersky
- Implementação de chaves de licença para os dispositivos cliente e armazenamento de informações sobre chaves de licença
- O encaminhamento de notificações sobre o progresso das tarefas (tal como detecção de vírus em um dispositivo cliente)

Nomeando Servidores de Administração na interface do aplicativo

Na interface do Kaspersky Security Center 14 Web Console, o servidor de administração pode ter os seguintes nomes:

- Nome do dispositivo do Servidor de Administração, por exemplo: "*nome do dispositivo*" ou "Servidor de Administração: *nome do dispositivo*".
- Endereço IP do dispositivo do Servidor de Administração, por exemplo: "*Endereço de IP*" ou "Servidor de Administração: *Endereço de IP*".
- Os Servidores de Administração secundários e virtuais têm nomes personalizados que você especifica ao conectar um Servidor de Administração virtual ou secundário ao Servidor de Administração principal.
- Se você usar o Kaspersky Security Center 14 Web Console: instalado em um dispositivo Linux, o aplicativo exibe os nomes dos Servidores de Administração especificados como confiáveis no [arquivo de resposta](#).

Você pode conectar-se ao Servidor de Administração por meio do Kaspersky Security Center 14 Web Console.

Hierarquia de Servidores de Administração

Os Servidores de Administração podem ser dispostos numa hierarquia principal/secundário. Cada Servidor de Administração pode possuir vários Servidores de Administração secundários (citados como *Servidores secundários*) em diferentes níveis de alojamento da hierarquia. O nível de alojamento para Servidores secundários não é limitado. Os grupos de administração do Servidor de Administração principal incluirão então os dispositivos cliente de todos os Servidores de Administração secundários. Portanto, as seções isoladas e independentes das redes podem ser gerenciadas por diferentes Servidores de Administração que, por sua vez, são gerenciadas pelo Servidor principal.

Os [Servidores de Administração virtuais](#) são um caso particular de Servidores de Administração secundários.

Em uma hierarquia, o Servidor de Administração Linux do Kaspersky Security Center só pode funcionar como um servidor secundário gerenciado por um Servidor de Administração principal do Kaspersky Security Center baseado em Windows ou do Kaspersky Security Center Cloud Console.

A hierarquia dos Servidores de Administração pode ser usada para o seguinte:

- Diminuir a carga no Servidor de Administração (em comparação com um único Servidor de Administração instalado para uma rede inteira).
- Diminuir o tráfego na intranet e simplificar o trabalho com escritórios remotos. Você não é precisa estabelecer conexões entre o Servidor de Administração principal e todos os dispositivos na rede, os quais podem estar localizados, por exemplo, em outras regiões. É suficiente para instalar em cada segmento de rede um Servidor de Administração secundário, distribuir dispositivos entre os grupos de administração de servidores secundários e estabelecer conexões entre os servidores secundários e o servidor principal em canais de comunicação rápida.
- Distribuir responsabilidades entre os administradores de segurança antivírus. Todos os recursos para gerenciamento e monitoramento centralizado do status de segurança antivírus em redes corporativas permanecem disponíveis.
- Como os provedores de serviço usam o Kaspersky Security Center. Um provedor de serviços somente necessita instalar o Kaspersky Security Center e o Kaspersky Security Center 14 Web Console. Para gerenciar um número maior de dispositivos cliente de várias organizações, um provedor de serviço pode adicionar Servidores de Administração virtuais à hierarquia de Servidores de Administração.

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 os recursos para a pesquisa de dispositivo em grupos de administração de diferentes Servidores 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 Linux projetado para gerenciar a proteção antivírus da rede de uma organização 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:

- O Servidor de Administração virtual só pode ser criado no Servidor de Administração principal.
- O Servidor de Administração virtual usa o banco de dados do Servidor de Administração principal. Tarefas de backup e restauração de dados, bem como tarefas de verificação de atualização e download, não são compatíveis com um Servidor de Administração virtual.
- O Servidor virtual não é compatível com a criação de Servidores de Administração secundários (incluindo Servidores virtuais).

Além disso, o Servidor de Administração virtual possui as seguintes restrições:

- Na janela de propriedades do Servidor de Administração virtual, o número de seções é limitado.
- Para instalar aplicativos Kaspersky remotamente em dispositivos cliente gerenciados pelo Servidor Administrativo virtual, você deve certificar-se de que o Agente de Rede está instalado em um dos dispositivos cliente para poder garantir a comunicação com o Servidor de Administração virtual. Na primeira conexão ao Servidor de Administração virtual, esse dispositivo é automaticamente atribuído como o ponto de distribuição, funcionando como um gateway de conexão entre os dispositivos cliente e o Servidor de Administração virtual.
- Um servidor virtual pode amostrar a rede somente através de pontos de distribuição.
- Para reiniciar um Servidor virtual que não está funcionando corretamente, o Kaspersky Security Center Linux reinicia o Servidor de Administração principal e todos os Servidores virtuais.

O administrador de um Servidor virtual possui todos os privilégios neste Servidor virtual em particular.

Servidor Web

O *Servidor Web* do Kaspersky Security Center (daqui em diante referido como *Servidor Web*) é um componente do Kaspersky Security Center que é instalado junto com o Servidor de Administração. O Servidor da Web foi projetado para a transmissão, através de uma rede, de pacotes de instalação independentes e arquivos de uma pasta compartilhada.

Ao criar um pacote de instalação independente, ela é automaticamente publicada no Servidor da Web. Um link para o download do pacote independente é exibido na lista de pacotes de instalação independentes criados. Se necessário, você poderá cancelar a publicação do pacote independente ou publicá-lo novamente no Servidor da Web.

A pasta compartilhada é usada para armazenar as informações que estão disponíveis para todos os usuários cujos dispositivos são gerenciados através do Servidor de Administração. Se um usuário não tiver acesso direto à pasta compartilhada, ele poderá receber informações a partir dessa pasta usando o Servidor da Web.

Para fornecer aos usuários informações da pasta compartilhada usando o Servidor da Web, o administrador deve criar uma subpasta com o nome de "pública" na pasta compartilhada e colar as informações nela.

A sintaxe do link de transferência de informações é a seguinte:

```
https://<Nome do Servidor d Web>:<Porta HTTPS>/public/<objeto>
```

onde:

- <nome do Servidor Web> é o nome do Servidor Web do Kaspersky Security Center.
- <porta HTTPS> é uma porta HTTPS do Servidor Web que foi definida pelo Administrador. A porta HTTPS pode ser definida na seção **Servidor da Web** da janela Propriedades do Servidor de Administração. O número da porta padrão é 8061.
- <objeto> é uma subpasta ou um arquivo ao qual o usuário tem acesso.

O administrador pode enviar o novo link ao usuário de qualquer forma prática: por exemplo, por e-mail.

Ao usar este link, o usuário poderá baixar as informações necessárias para um dispositivo local.

Agente de Rede

A interação entre o Servidor de Administração e os dispositivos é realizada pelo componente *Agente de Rede* do Kaspersky Security Center. O Agente de Rede deve ser instalado em todos os dispositivos cliente, nos quais o Kaspersky Security Center é usado para gerenciar os aplicativos 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 Linux"
- 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 de uma das seguintes fontes:

- Pacote de instalação no armazenamento do Servidor de Administração (você precisa ter o Servidor de Administração instalado)
- Pacote de instalação localizado nos servidores da web Kaspersky

Você não precisa instalar o Agente de Rede no dispositivo onde instalou o Servidor de Administração, porque a versão de servidor do Agente de Rede é automaticamente instalada em conjunto com o Servidor de Administração.

Os nomes do processo que o Agente de Rede inicia são:

- `klagent64.service` (para um sistema operacional de 64 bits)
- `klagent.service` (para um sistema operacional de 32 bits)

O Agente de Rede sincroniza o dispositivo gerenciado com o Servidor de Administração. Recomendamos definir o intervalo de sincronização (também conhecido como *heartbeat*) para 15 minutos a cada 10.000 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.

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.

Dispositivo gerenciado

Um *dispositivo gerenciado* é um computador que executa Linux e que tem o Agente de Rede instalado. Você pode gerenciar esses dispositivos criando tarefas e políticas para os aplicativos instalados nos dispositivos. Você também pode receber relatórios dos dispositivos gerenciados.

Você pode transformar uma função de dispositivo gerenciado em um ponto de distribuição e em um gateway de conexão.

Um dispositivo pode ser gerenciado somente por um Servidor de Administração. Um Servidor de Administração pode gerenciar até 20.000 dispositivos.

Dispositivo não atribuído

Um *dispositivo não atribuído* é um dispositivo na rede que não estava incluído em nenhum grupo de administração. Você pode executar algumas ações em dispositivos não atribuídos, por exemplo, movê-los para seus grupos de administração ou instalar aplicativos neles.

Quando um novo dispositivo é descoberto na rede, esse dispositivo vai para o grupo de administração Dispositivos não atribuídos. Você pode configurar regras para que os dispositivos sejam movidos automaticamente para outros grupos de administração após serem descobertos.

Estação de trabalho do administrador

Os dispositivos nos quais o Kaspersky Security Center 14 Web Console Server está instalado, são referidos como *estações de trabalho do administrador*. Os administradores podem usar esses dispositivos para o gerenciamento remoto centralizado dos aplicativos Kaspersky instalados nos dispositivos cliente.

Não há restrições quanto ao número de estações de trabalho do administrador. Em qualquer estação de trabalho do administrador, você pode gerenciar os grupos de administração de vários Servidores de Administração na rede de uma só vez. Você pode conectar uma estação de trabalho do administrador a um Servidor de Administração (físico ou virtual) de qualquer nível de hierarquia.

Você pode incluir uma estação de trabalho do administrador em um grupo de administração como um dispositivo cliente.

Dentro dos grupos de administração de qualquer Servidor de Administração, o mesmo dispositivo pode funcionar como um Servidor de Administração cliente, um Servidor de Administração ou uma estação de trabalho do administrador.

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 14 Web Console. No presente documento, o plug-in da Web de gerenciamento será referido como *plug-in de gerenciamento*. Um plug-in de gerenciamento é uma interface entre o Kaspersky Security Center 14 Web Console e um aplicativo da Kaspersky específico. Com um plug-in de gerenciamento, você pode configurar tarefas e políticas para o aplicativo.

É possível baixar plug-ins de gerenciamento da web a partir da [página de Serviço ao Cliente da Kaspersky](#).

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 14 Web Console para exibir os dados operacionais e os eventos do aplicativo, além das estatísticas transmitidas de 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 fornece uma única política para cada aplicativo Kaspersky em um grupo de administração. Uma política possui um dos seguintes status:

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.
Inativa	Uma política que não é aplicada atualmente a um dispositivo.
Remota	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.
- 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 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 ajudá-lo a evitar a criação de várias instâncias de uma única política, o Kaspersky Security Center 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.

Tarefas

O Kaspersky Security Center gerencia os aplicativos de segurança da 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 de um aplicativo específico podem ser criadas apenas se o plugin de gerenciamento desse aplicativo estiver instalado.

As tarefas podem ser realizadas no Servidor de Administração e em dispositivos.

As seguintes tarefas que são realizadas no Servidor de Administração:

- Distribuição automática de relatórios
- Baixar atualizações no repositório do Servidor de Administração
- Backup de dados do Servidor de Administração
- Manutenção do banco de dados
- Criação de um pacote de instalação com base na imagem do sistema operacional (SO) de um dispositivo de referência

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 o Kaspersky Security Center 14 Web Console ou por um usuário de um dispositivo remoto (por exemplo, por meio 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. Uma tarefa de grupo também afeta (opcionalmente) os dispositivos que foram conectados aos Servidores de Administração secundários e virtuais implementados no grupo ou em algum dos seus subgrupos.

- *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 qualquer número de 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 das tarefas são salvos no log de eventos do Syslog e no [log de eventos do Kaspersky Security Center](#), tanto centralmente no Servidor de Administração como localmente em cada dispositivo.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Escopo da 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) 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.

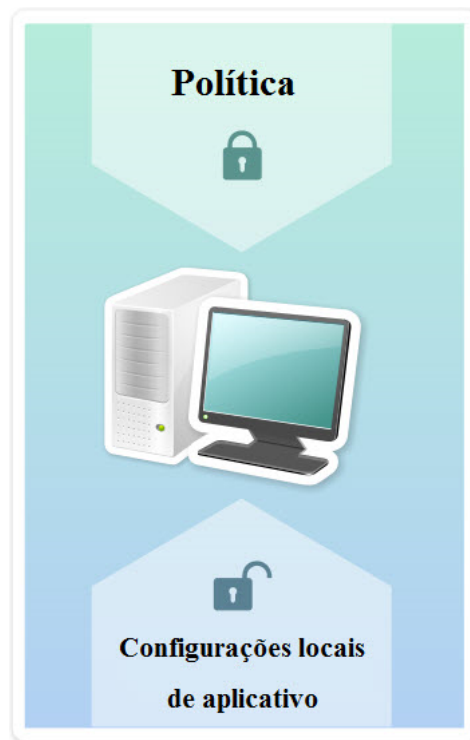
Como as configurações do aplicativo local se relacionam com as políticas

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 (veja a figura abaixo) é definido pela posição do bloqueio (🔒) 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.



Política e configurações de aplicativos 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 aplicativos locais são alteradas depois da primeira imposição de política de acordo com as configurações de política.

Ponto de distribuição

Ponto de distribuição (anteriormente conhecido como agente de atualização) 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 do Servidor de Administração para os dispositivos cliente no grupo (incluindo a distribuição por meio de multicasting usando UDP). As atualizações podem ser recebidas do Servidor de Administração ou dos servidores de atualização Kaspersky. Nesse caso, uma tarefa de atualização precisa ser criada para o ponto de distribuição.

Os pontos de distribuição agilizam a distribuição da atualização e permite liberar recursos do Servidor de Administração.

- 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. Um ponto de distribuição pode aplicar os mesmos métodos de localização dos dispositivos que os do Servidor de Administração.
- Execute a instalação remota de aplicativos pela Kaspersky e outros fornecedores de software, incluindo a instalação em dispositivos clientes sem o Agente de Rede.

Esse 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.

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.

Aos dispositivos com o Agente de Rede instalado podem ser atribuídos pontos de distribuição de forma manual (pelo administrador) ou automaticamente (pelo Servidor 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. 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.

Se os pontos de distribuição forem automaticamente atribuídos pelo Servidor de Administração, ele os atribui por domínios de difusão, não por grupos de administração. Isso ocorre quando todos os domínios de difusão são conhecidos. O Agente de Rede troca mensagens com outros Agentes de Rede na mesma sub-rede e, a seguir, envia informações ao Servidor de Administração sobre si mesmo e de outros Agentes de Rede. O Servidor de Administração usa estas informações para agrupar os Agentes de atualização por domínios de difusão. Os domínios de difusão são conhecidos para o Servidor de Administração após mais de 70% dos Agentes de rede nos grupos de administração forem amostrados. O Servidor de Administração efetua a sondagem dos domínios de difusão a cada duas horas. Após os pontos de distribuição terem sido atribuídos pelo domínio de difusão, eles não podem ser reatribuídos por grupos de administração.

Se o administrador atribuir manualmente pontos de distribuição, eles poderão ser atribuídos a grupos de administração ou locais de rede.

Os Agentes de Rede com um perfil de conexão ativo não participam na detecção do domínio de difusão.

O Kaspersky Security Center Linux atribui a cada Agente de Rede um endereço IP multicast único que se diferencia de cada outro endereço. Isto lhe permite evitar a sobrecarga de rede que poderia ocorrer devido a sobreposições de IP. Os endereços IP multicast que foram atribuídos em versões anteriores do aplicativo não serão modificados.

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. Se o espaço disponível livre do ponto de distribuição for menor do que 2 GB, o Kaspersky Security Center Linux cria um incidente com o nível de importância *Aviso*. O incidente será publicado nas propriedades do dispositivo, na seção **Incidentes**.

Executar tarefas de instalação remota em um dispositivo atribuído como ponto de distribuição exige espaço livre adicional no disco. O volume do espaço em disco disponível livre deve exceder o tamanho total de todos os pacotes de instalação a ser instalados.

Executar qualquer tarefa de atualização (patch) e de correção de vulnerabilidades em um dispositivo atribuído como ponto de distribuição exige espaço livre adicional no disco. 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.

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.

Um gateway de conexão pode receber conexões de até 10.000 dispositivos.

Você tem duas opções para usar gateways de conexão:

- Recomendamos instalar um gateway de conexão em uma zona desmilitarizada (DMZ). Para outros Agentes de Rede instalados em dispositivos externos, você precisa configurar especialmente uma conexão ao Servidor de Administração por meio do gateway de conexão.

Um gateway de conexão não modifica ou processa de forma alguma os dados transmitidos dos Agentes de Rede para o Servidor de Administração. Além disso, ele não grava esses dados em nenhum buffer e, portanto, não pode aceitar dados de um Agente de Rede e posteriormente encaminhá-los ao Servidor de Administração. Se o Agente de Rede tentar se conectar ao Servidor de Administração através do gateway de conexão, mas esse não puder se conectar ao Servidor de Administração, o Agente de Rede interpretará isso como se o Servidor de Administração estivesse inacessível. Todos os dados permanecem no Agente de Rede (não no gateway de conexão).

Um gateway de conexão não pode se conectar ao Servidor de Administração por meio de outro gateway de conexão. Isso significa que o Agente de Rede não pode ser simultaneamente um gateway de conexão e usar um gateway de conexão para se conectar ao Servidor de Administração.

Todos os gateways de conexão estão incluídos na lista de pontos de distribuição nas propriedades do Servidor de Administração.

- Você também pode usar gateways de conexão dentro da rede. Por exemplo, pontos de distribuição atribuídos automaticamente também se tornam gateways de conexão em seu próprio escopo. No entanto, em uma rede interna, os gateways de conexão não oferecem benefícios consideráveis. Eles reduzem o número de conexões de rede recebidas pelo Servidor de Administração, mas não reduzem o volume de dados de entrada. Mesmo sem gateways de conexão, todos os dispositivos ainda podem se conectar ao Servidor de Administração.

Licenciamento

Esta seção traz informações sobre os termos gerais relacionados à licença do Kaspersky Security Center 14 Linux.

Sobre o Contrato de Licença do Usuário Final

O *Contrato de Licença do Usuário Final* (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.

Leia com atenção o seguinte Contrato de Licença antes de começar a usar o aplicativo.

O Kaspersky Security Center Linux e seus componentes, por exemplo, Agente de Rede, têm seu próprio EULA.

Você pode visualizar os termos do Contrato de Licença do Usuário Final para o Kaspersky Security Center Linux usando os seguintes métodos:

- Durante a instalação do Kaspersky Security Center.
- Lendo o documento `license.txt` incluído no kit de distribuição do Kaspersky Security Center.
- Lendo o documento `license.txt` presente na pasta de instalação do Kaspersky Security Center.

Você pode visualizar os termos do Contrato de Licença do Usuário Final para o Agente de Rede para Linux usando os seguintes métodos:

- Durante o download do pacote de distribuição do Agente de Rede dos servidores da web Kaspersky.
- Durante a instalação do Agente de Rede para Linux.

Observe que quando você instala o Agente de Rede para Linux, o Contrato de Licença do Usuário Final do Agente de Rede é exibido em inglês. Você pode verificar o Contrato de Licença do Usuário Final para Agente de Rede em outros idiomas na pasta `/opt/kaspersky/klnagent64/share/license` antes de aceitar os termos do Contrato de Licença do Usuário Final durante a instalação.

- Lendo o documento `license.txt` incluído no pacote de distribuição do Agente de Rede para Linux.
- Lendo o documento `license.txt` constante na pasta de instalação do Agente de Rede para Linux.

Você aceita os termos do Contrato de Licença do Usuário Final confirmando que concorda com o Contrato de Licença do Usuário Final ao instalar o aplicativo. Se você não aceitar os termos do Contrato de Licença, cancele a instalação do aplicativo e não o utilize.

Sobre a licença

Uma *licença* é um direito com período de validade limitado para uso do aplicativo, concedido nos termos do Contrato de Licença do Usuário Final.

Uma licença lhe dá o direito de usar os seguintes tipos de serviços:

- O uso do aplicativo de acordo com os termos do Contrato de Licença de Usuário Final.
- Obtenção de Suporte Técnico.

O escopo dos serviços e o período de validade dependem do tipo de licença sob a qual o aplicativo foi ativado.

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 a licença de avaliação expira, todos os recursos do Kaspersky Security Center Linux são desativados. Para continuar usando o aplicativo, você precisa comprar a licença comercial.

Você pode ativar o aplicativo com a licença de avaliação somente uma vez.

- *Comercial* – uma licença paga, concedida mediante a compra do aplicativo.

Quando a licença comercial expira, o aplicativo continua em execução com funcionalidade limitada (por exemplo, as atualizações do banco de dados do Kaspersky Security Center não estarão disponíveis). Para continuar usando todos os recursos do Kaspersky Security Center, você deve renovar sua licença.

Recomendamos a renovação da 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.

Você pode adicionar uma chave de licença ao aplicativo usando um dos seguintes métodos: aplicando um *arquivo de chave* ou 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.

Ler a Política de Privacidade

A Política de Privacidade está disponível on-line em <https://www.kaspersky.com/products-and-services-privacy-policy>.

A Política de Privacidade também está disponível off-line:

- Você pode ler a Política de Privacidade antes [instalando o Kaspersky Security Center](#).
- O texto da Política de Privacidade está incluído no arquivo license.txt, na pasta de instalação do Kaspersky Security Center.
- O arquivo privacy_policy.txt está disponível em um dispositivo gerenciado, na pasta de instalação do Agente de Rede.
- Você pode descompactar o arquivo privacy_policy.txt do pacote de distribuição do Agente de Rede.

Opções de licença do Kaspersky Security Center

O Kaspersky Security Center é fornecido como parte dos aplicativos Kaspersky para proteção de redes corporativas. Você também pode baixá-lo no [site da Kaspersky](#).

As seguintes funções estão disponíveis:

- Criação de Servidores de Administração virtuais para gerenciar uma rede de escritórios remotos ou organizações clientes
- Criação de uma hierarquia de grupos de administração para gerenciar dispositivos específicos como uma entidade única
- Controle do status de segurança antivírus de uma organização

- Instalação remota de aplicativos
- Visualização da lista de imagens do sistema operacional disponíveis para instalação remota
- Configuração centralizada de aplicativos instalados em dispositivos cliente
- Exibir e editar grupos de aplicativos licenciados existentes
- Estatísticas e relatórios sobre a operação do aplicativo assim como notificações sobre eventos críticos
- Visualização e edição manual da lista de componentes de hardware detectados pela sondagem da rede
- Operações centralizadas com arquivos que foram movidos para a Quarentena e Backup e arquivos cujo processamento foi adiado
- Gerenciamento de funções do usuário

Sobre o arquivo de chave

Um *arquivo de chave* é um arquivo com a extensão .key fornecido a você pela Kaspersky. Os arquivos de chave se destinam a ativar o aplicativo adicionando uma chave de licença.

Você recebe o arquivo de chave pelo endereço de e-mail que especificou após comprar o Kaspersky Security Center, ou que utilizou para solicitar a versão de avaliação do Kaspersky Security Center.

Você não precisa se conectar aos servidores de ativação da Kaspersky para ativar o aplicativo com um arquivo de chave.

Você pode recuperar um arquivo de chave se ele tiver sido acidentalmente excluído. Você poderá precisar de um arquivo de chave para se registrar no Kaspersky CompanyAccount, por exemplo.

Para restaurar seu arquivo de chave, realize uma das seguintes ações:

- Entre em contato com o vendedor da licença.
- Receba um arquivo de chave através do [site da Kaspersky](#) usando o código de ativação.

Sobre a coleta de dados

Dados transferidos para o Titular dos direitos

Fornecido no Contrato de Licença do Usuário Final do Kaspersky Security Center 14 Linux.

Dados processados localmente

O Kaspersky Security Center Linux foi projetado para a execução centralizada de administração básica e tarefas de manutenção em uma rede corporativa. O Kaspersky Security Center Linux fornece ao administrador o acesso a informações detalhadas sobre o nível de segurança da rede corporativa. O Kaspersky Security Center 13 Linux permite ao administrador configurar todos os componentes de proteção criados com base nos aplicativos Kaspersky. O Kaspersky Security Center Linux executa as seguintes funções principais:

- Detecção de dispositivos e seus usuários na rede da organização
- Criação de uma hierarquia de grupos administrativos para gerenciamento de dispositivos
- Instalação de aplicativos da Kaspersky nos dispositivos
- Gerenciamento de configurações e tarefas dos aplicativos instalados
- Ativação de aplicativos da Kaspersky nos dispositivos
- Como gerenciar contas de usuário
- Visualizando informações sobre a operação dos aplicativos da Kaspersky nos dispositivos
- Visualização de relatórios

Para desempenhar sua função principal, o Kaspersky Security Center Linux pode receber, armazenar e processar as seguintes informações:

- Informações sobre os dispositivos na rede da organização recebidas como resultado da detecção de dispositivos na rede, através da verificação de intervalos de IP. O Servidor de Administração obtém dados por conta própria ou recebe dados do Agente de Rede.
- 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 14 Web Console:
 - Especificações técnicas do dispositivo gerenciado e de seus componentes requeridos para identificação do dispositivo: nome de exibição e descrição do dispositivo, domínio e nome DNS, endereço IPv4, endereço IPv6, local da rede, endereço MAC, tipo de sistema operacional, se o dispositivo é uma máquina virtual junto com o tipo de hipervisor e se o dispositivo é uma máquina virtual dinâmica como parte da VDI.
 - Outras especificações de dispositivos gerenciados e os componentes necessários para auditoria de dispositivos gerenciados: arquitetura do sistema operacional, fornecedor do sistema operacional, número da compilação do sistema operacional, ID da versão do sistema operacional, pasta de localização do sistema operacional, se o dispositivo é uma máquina virtual, o tipo de máquina virtual.
 - Detalhes de ações em dispositivos gerenciados: data e hora da última atualização, hora em que o dispositivo esteve visível na rede pela última vez, status de espera de reinício e hora em que o dispositivo foi ligado.
 - Detalhes das contas de usuário do dispositivo e as suas sessões.
- Estatísticas de operação do ponto de distribuição se o dispositivo for um ponto de distribuição. O Agente de Rede transfere os dados do dispositivo para o Servidor de Administração.
- Configurações do ponto de distribuição inseridas pelo usuário no Kaspersky Security Center 14 Web Console.
- 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:

- Configurações dos aplicativos da 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 com falha na desinfecção, disponibilidade e status dos componentes do aplicativo, detalhes sobre as configurações e tarefas do aplicativo da Kaspersky, informações sobre chaves de licença ativa e adicional, data e ID de instalação.
- Estatística da operação de aplicativo: eventos relacionados a alterações no status dos componentes do aplicativo da Kaspersky no dispositivo gerenciado e desempenho de tarefas iniciadas pelos componentes de software.
- Status do dispositivo definido pelo aplicativo da Kaspersky.
- Marcações feitas por o aplicativo da Kaspersky.
- Dados contidos em eventos dos componentes do Kaspersky Security Center Linux e aplicativos gerenciados Kaspersky. O Agente de Rede transfere os dados do dispositivo para o Servidor de Administração.
- Configurações dos componentes do Kaspersky Security Center Linux e Kaspersky gerenciados estão disponíveis nas políticas e nos perfis das políticas. O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- Configurações de tarefas dos componentes do Kaspersky Security Center Linux e aplicativos gerenciados Kaspersky. O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- Dados processados pelo recurso de Gerenciamento de Patches e Vulnerabilidades. O Agente de Rede transfere informações contidas no Servidor de Administração sobre hardware detectado em dispositivos gerenciados (registro de hardware).
- Categorias de usuários de aplicativos. O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- Detalhes de arquivos executáveis detectados em dispositivos gerenciados pelo recurso de Controle de Aplicativos. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Detalhes sobre arquivos colocados em Backup. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Detalhes sobre arquivos colocados em Quarentena. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Detalhes sobre arquivos requisitados por especialistas da Kaspersky para análise detalhadas. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Detalhes sobre dispositivos externos (unidades de memória, ferramentas de transferência de informações, ferramentas de cópia impressa de informações e conexões de buses) instalados ou conectados ao dispositivo gerenciado e detectados pelo recurso de Controle de Dispositivos. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Lista de controladores lógicos programáveis (PLCs) gerenciados. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Detalhes dos códigos de ativação inseridos. O usuário insere dados no Console de Administração ou no Kaspersky Security Center 14 Web Console.
- Contas de usuários: nome, descrição, nome completo, endereço de e-mail, telefone principal, e senha. O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- Revisão de histórico de objetos gerenciados excluídos. O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- Registro de objetos gerenciados excluídos. O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- Pacotes de instalação criados dos arquivos e configurações de instalações. O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- Dados necessários para a exibição de informativos da Kaspersky no Kaspersky Security Center 14 Web Console. O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- Dados necessários para o funcionamento de plugins de aplicativos gerenciados no Kaspersky Security Center 14 Web Console e salvos pelos plugins no banco de dados do Servidor de Administração durante sua operação de rotina. A descrição e formas de fornecer os dados são fornecidas nos arquivos de Ajuda do aplicativo correspondente.
- Configurações de usuário do Kaspersky Security Center 14 Web Console: idioma de localização e tema da interface, configurações de exibição do painel de monitoramento, informações sobre o status das notificações (Já lidas/Ainda não lidas), status das colunas nas planilhas (Mostrar/Ocultar), Modo de treinamento progresso. O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- Log de Eventos Kaspersky para os componentes do Kaspersky Security Center Linux e para o aplicativo gerenciado Kaspersky. O Log de eventos Kaspersky é armazenado em cada dispositivo e nunca é transferido para o Servidor de Administração.
- Certificados de comunicação segura dos dispositivos gerenciados e componentes do Kaspersky Security Center Linux. O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- Os dados do Servidor de Administração inseridos pelo usuário no Kaspersky Security Center 14 Web Console.
- Quaisquer dados inseridos pelo usuário na interface do Kaspersky Security Center 14 Web Console.

Os dados listados acima podem estar presentes no Kaspersky Security Center Linux se um dos seguintes métodos for aplicado:

- O usuário insere dados na interface do Kaspersky Security Center 14 Web Console.
- O Agente de Rede automaticamente recebe dados do dispositivo e os transfere para o Servidor de Administração.
- 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 por aplicativos gerenciados do Kaspersky são providenciados nos arquivos de Ajuda para os aplicativos correspondentes.
- O Servidor de Administração e o Agente de Rede atribuídos a um ponto de distribuição recebem informações sobre os dispositivos em rede.

Os dados são armazenados no banco de dados do Servidor de Administração. Os nomes de usuários e as senhas são armazenados em formato criptografado.

Todos os dados processados localmente podem ser transferidos para a Kaspersky apenas através de arquivos de dumping, arquivos de rastreamento ou arquivos de log dos componentes do Kaspersky Security Center Linux, incluindo arquivos de log criados por instaladores e utilitários.

A Kaspersky protege todas as informações recebidas, seguindo as leis e regras aplicáveis da Kaspersky. Os dados são transmitidos através de um canal seguro.

Seguindo os links no Console de Administração ou Kaspersky Security Center 14 Web Console, o usuário concorda com a transferência automática dos seguintes dados:

- Código do Kaspersky Security Center Linux
- Versão do Kaspersky Security Center Linux
- Localização do Kaspersky Security Center Linux
- ID da licença
- Tipo de 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.

A Kaspersky usa a informação recebida de forma anônima e somente como estatística geral. O resumo das estatísticas é gerado automaticamente através da informação original recebida e não contém qualquer dado pessoal ou confidencial. Assim que os dados novos são acumulados, os dados anteriores são excluídos (uma vez por ano). As estatísticas sumarizadas são armazenadas por tempo indeterminado.

Sobre a assinatura

A *Assinatura para o Kaspersky Security Center Linux* 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 Linux 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 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 Linux 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 Linux 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.

Ao usar o aplicativo sob a assinatura, o Kaspersky Security Center Linux automaticamente tenta acessar o servidor de ativação em intervalos de tempo especificados até que a assinatura expire. Você pode renovar sua assinatura no site do provedor de serviços.

Eventos do limite do licenciamento excedidos

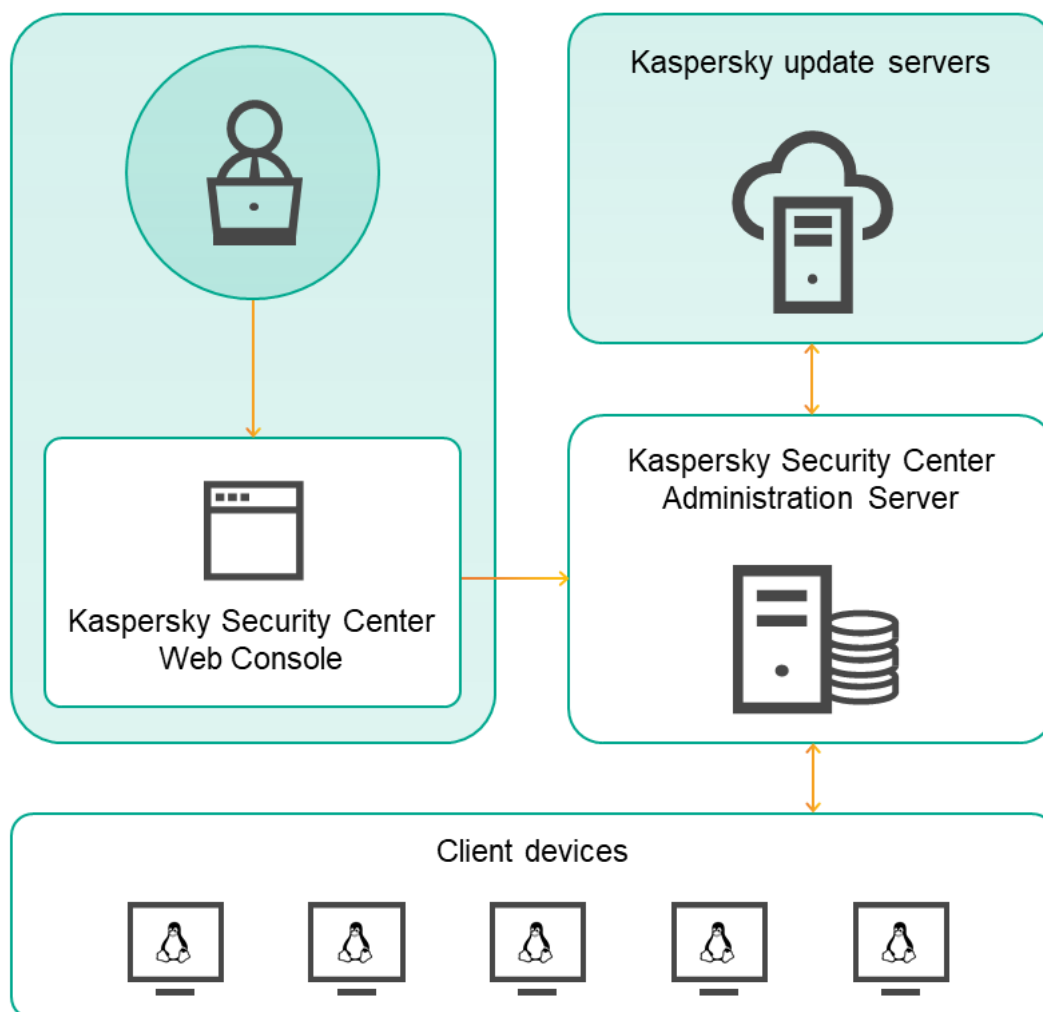
O Kaspersky Security Center Linux lhe permite obter informações sobre eventos quando alguns limites de licenciamento são excedidos pelos aplicativos da Kaspersky instalados nos dispositivos cliente.

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**.

Arquitetura

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



Arquitetura do Kaspersky Security Center 14 Linux

O Kaspersky Security Center 14 Linux inclui os seguintes componentes básicos:

- **Kaspersky Security Center Web Console.** Fornece uma interface Web para criar e manter o sistema de proteção da rede de uma organização cliente gerenciada pelo Kaspersky Security Center.
- **Servidor de Administração do Kaspersky Security Center** (também chamado de *Servidor*). Centraliza o armazenamento das informações sobre os aplicativos instalados na rede da organização e a forma como é possível gerenciá-los.
- **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 da KSN.** Servidores que contêm informações o 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.
- **Dispositivos cliente.** Dispositivos cliente da empresa, protegidos pelo Kaspersky Security Center 14 Linux. Cada dispositivo que precisa ser protegido deve ter um dos aplicativos de segurança Kaspersky instalados.

Diagrama de implementação do Servidor de Administração do Kaspersky Security Center e do Kaspersky Security Center 14 Web Console

A figura abaixo mostra o diagrama de implementação do Servidor de Administração do Kaspersky Security Center e do Kaspersky Security Center 14 Web Console.

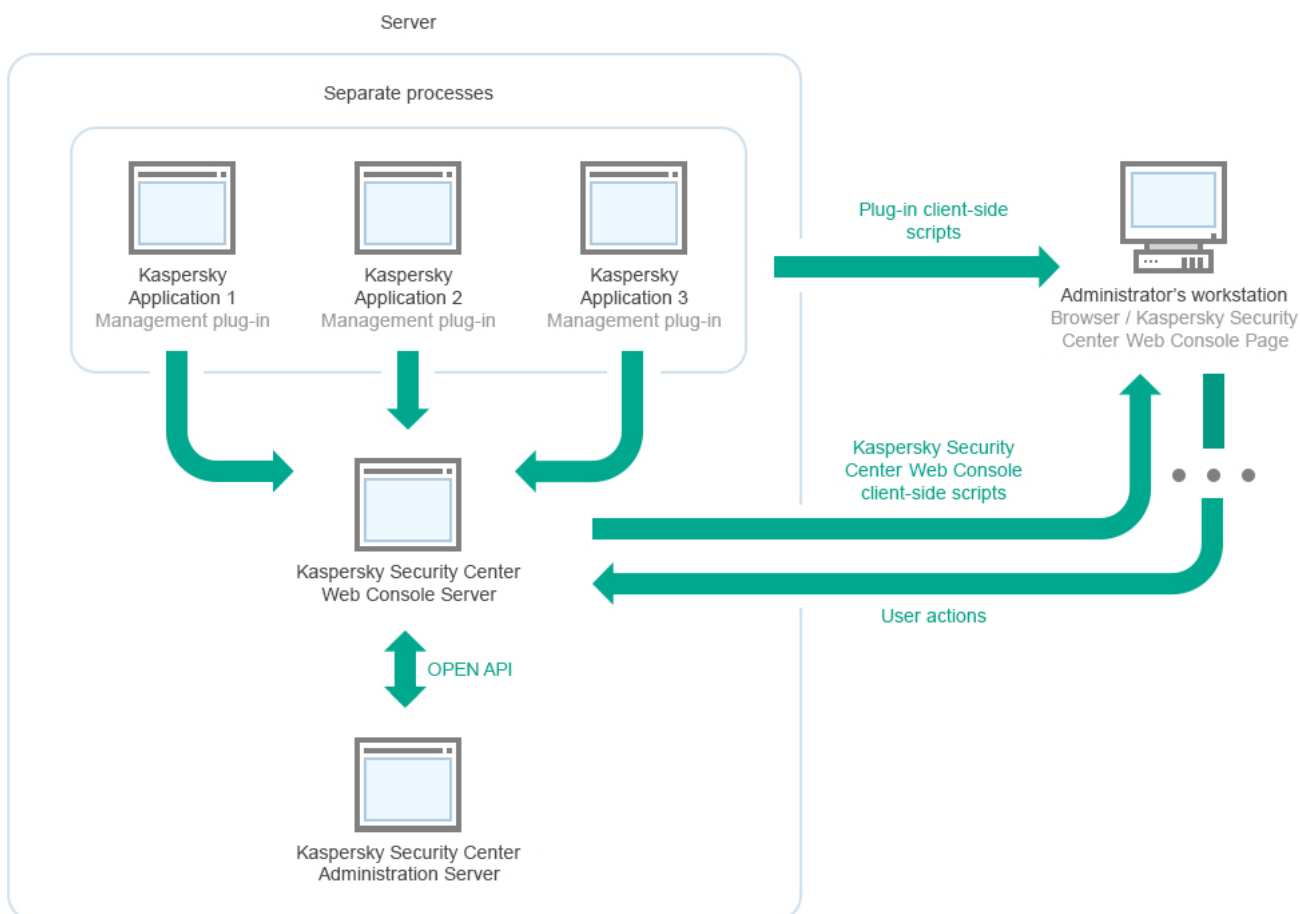


Diagrama de implementação do Servidor de Administração do Kaspersky Security Center e do Kaspersky Security Center 14 Web Console

Os plug-ins de gerenciamento para aplicativos Kaspersky instalados em dispositivos protegidos (um plugin para cada aplicativo) são implementados em conjunto com o Kaspersky Security Center 14 Web Console Server.

Como administrador, você acessa o Kaspersky Security Center 14 Web Console usando um navegador na sua estação de trabalho.

Quando você executa ações específicas no Kaspersky Security Center 14 Web Console, o Kaspersky Security Center 14 Web Console Server se comunica com o Servidor de Administração do Kaspersky Security Center por meio do OpenAPI. O Kaspersky Security Center 14 Web Console Server solicita as informações necessárias do Servidor de Administração do Kaspersky Security Center e exibe os resultados das operações no Kaspersky Security Center 14 Web Console.

Portas usadas pelo Kaspersky Security Center Linux

As tabelas abaixo mostram as portas padrão que devem estar abertas no servidor de administração e em dispositivos cliente. Se desejar, você pode alterar cada um desses números de porta padrão.

Portas utilizadas pelo servidor de Administração do Kaspersky Security Center Linux

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
8060	klcsweb	TCP	Transmitindo pacotes de instalação publicados aos dispositivos cliente	Publicando pacotes de instalação. Você pode alterar o número da porta padrão na seção Servidor da Web da janela Propriedades do Servidor de Administração.
8061	klcsweb	TCP (TLS)	Transmitindo pacotes de instalação publicados aos dispositivos cliente	Publicando pacotes de instalação. Você pode alterar o número da porta padrão na seção Servidor da Web da janela Propriedades do Servidor de Administração.
13000	klserver	TCP (TLS)	Receber conexões de Agentes de Rede e Servidores de Administração secundários; também usado em Servidores de Administração secundários para receber conexões do Servidor de Administração principal (por exemplo, se o Servidor de Administração secundário estiver na DMZ)	Gerenciando dispositivos cliente e Servidores de Administração secundários. É possível alterar o número da porta padrão para receber conexões dos Agentes de Rede ao configurar portas de conexão durante a instalação do Kaspersky Security Center Linux. É possível alterar o número da porta padrão para receber conexões de Servidores de Administração secundários ao criar uma hierarquia de Servidores de Administração .
13000	klserver	UDP	Recebendo informações sobre dispositivos que foram desativados a partir de Agentes de Rede	Gerenciando dispositivos cliente. Você pode alterar o número da porta padrão na janela nas Configurações de política do Agente de Rede .
13299	klserver	TCP (TLS)	Receber conexões do Kaspersky Security Center 14 Web Console para o Servidor de Administração; receber conexões para o Servidor de Administração através do OpenAPI	Kaspersky Security Center 14 Web Console, OpenAPI. É possível alterar o número da porta padrão na janela de propriedades do Servidor de Administração (na subseção Portas de conexão da seção Geral) ou ao criar uma hierarquia de Servidores de Administração .
14000	klserver	TCP	Receber conexões dos Agentes de Rede	Gerenciando dispositivos cliente.

				É possível alterar o número da porta padrão ao configurar portas de conexão durante a instalação do Kaspersky Security Center Linux ou ao conectar manualmente um dispositivo cliente ao Servidor de Administração .
13111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	TCP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. Você pode alterar o número da porta padrão na janela Propriedades do Servidor de Administração.
15111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	UDP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. Você pode alterar o número da porta padrão na janela Propriedades do Servidor de Administração.
17000	klactprx	TCP (TLS)	Recebendo conexões de dispositivos gerenciados para a ativação do aplicativo	Servidor proxy de ativação para dispositivos gerenciados. Você pode alterar o número da porta padrão na janela de propriedades do Servidor de Administração (na subseção Portas adicionais da seção Geral).
19170	klserver	HTTPS (TLS)	Tunelamento das conexões com dispositivos gerenciados usando o utilitário klsc tunnel	Fazendo a conexão remota a dispositivos gerenciados usando o Kaspersky Security Center 14 Web Console. É possível alterar o número da porta padrão usando o utilitário klscflag.

Se você instalar o Servidor de Administração e o banco de dados em dispositivos diferentes, deverá disponibilizar as portas necessárias no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MariaDB Server). Consulte a documentação do DBMS para obter informações relevantes.

A tabela abaixo mostra a porta que deve ser aberta no servidor do Kaspersky Security Center Linux Web Console. Pode ser o mesmo dispositivo no qual o Servidor de Administração está instalado ou em outro.

Porta usada pelo Kaspersky Security Center Linux Web Console

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
8080	Node.js: JavaScript do lado do servidor	TCP (TLS)	Receber conexões do navegador no Kaspersky	Kaspersky Security Center 14 Web Console.

			Security Center 14 Web Console	É possível alterar o número da porta padrão ao instalar o Kaspersky Security Center 14 Web Console . Ao instalar o Kaspersky Security Center 14 Web Console no sistema operacional Linux ALT, é necessário especificar um número de porta diferente de 8080, pois essa porta é usada pelo sistema operacional.
--	--	--	--------------------------------	--

A tabela abaixo mostra a porta que deve ser aberta em dispositivos gerenciados onde o Agente de Rede está instalado.

Portas usadas pelo Agente de Rede

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
15000	klnagent	UDP	Sinais de gerenciamento do Servidor de Administração para os Agentes de Rede	Gerenciando dispositivos cliente. Você pode alterar o número da porta padrão na janela nas Configurações de política do Agente de Rede .
15000	klnagent	Transmissão UDP	Obtendo dados sobre outros Agentes de Rede no mesmo domínio de transmissão (os dados são enviados ao Servidor de Administração)	Fornecendo atualizações e pacotes de instalação.
15001	klnagent	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. Você pode alterar o número da porta padrão na janela propriedades do ponto de distribuição .

A tabela abaixo mostra as portas que devem ser abertas em um dispositivo gerenciado com o Agente de Rede instalado atuando como um ponto de distribuição. As portas listadas devem estar abertas nos dispositivos do ponto de distribuição, além das portas usadas pelos Agentes de Rede (consulte a tabela acima).

Portas usadas pelo Agente de Rede funcionando como ponto de distribuição

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
13000	klnagent	TCP (TLS)	Receber conexões dos Agentes de Rede	Gerenciar dispositivos cliente, entregar atualizações e pacotes de instalação. É possível alterar o número da porta padrão nas propriedades do ponto de distribuição .
13111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	TCP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN.

				É possível alterar o número da porta padrão nas propriedades do ponto de distribuição .
15111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	UDP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. É possível alterar o número da porta padrão nas propriedades do ponto de distribuição .

Portas usadas pelo Kaspersky Security Center 14 Web Console

A tabela abaixo lista as portas que devem estar abertas no dispositivo em que o Servidor do Kaspersky Security Center 14 Web Console (também chamado de Kaspersky Security Center 14 Web Console) está instalado.

Portas usadas pelo Kaspersky Security Center 14 Web Console

Número da porta	Nome do serviço	Protocolo	Propósito da porta	Es
2001	KSCWebConsolePlugin	HTTPS	Porta da API que é usada pelos processos de plug-in de gerenciamento para receber solicitações do KSCWebConsoleManagementService	Execut proces node.e plugins gerenc
1329, 2003	KSCWebConsoleManagementService	HTTPS	Portas da API usadas para receber solicitações do serviço KSCWebConsole em execução no mesmo dispositivo	Atualiz compo do Kas Securi Cente Consc
2005	KSCWebConsole	HTTPS	Porta da API usada para receber solicitações do serviço KSCWebConsoleManagementService em execução no mesmo dispositivo	Execut proces node.e Kasper Securi Cente Consc
8200	—	HTTP	Porta API usada para gerar certificados por meio do HashiCorp Vault (para mais detalhes, consulte o site do HashiCorp Vault)	Instala Kasper Securi Cente Consc atualiz compo do Kas Securi Cente Consc
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	Portas API do processador de mensagens usadas para comunicação entre processos do Kaspersky Security Center 14 Web Console e plugins de gerenciamento	Interaç proces entre Kasper Securi Cente Consc plugins gerenc

Instalação

Esta seção descreve a instalação do Kaspersky Security Center e do Kaspersky Security Center 14 Web Console.

Cenário principal de implementação

Seguindo este cenário, você pode instalar o Servidor de Administração do Kaspersky Security Center 14 Linux e o Kaspersky Security Center 14 Web Console, executar a configuração inicial do Servidor de Administração usando o Assistente de Início Rápido e instalar aplicativos Kaspersky nos dispositivos gerenciados usando o Assistente de Implementação da Proteção.

Pré-requisitos

Você deve ter uma chave de licença (código de ativação) para o Kaspersky Endpoint Security for Business ou chaves de licença (códigos de ativação) para os aplicativos de segurança Kaspersky.

Se deseja primeiro testar o Kaspersky Security Center 14 Linux pode obter uma avaliação gratuita de 30 dias no [site da Kaspersky](#).

Fases

O cenário principal de implementação ocorre nas seguintes fases:

1 Selecionar uma estrutura para a proteção de uma organização

[Saiba mais sobre os componentes do Kaspersky Security Center Linux](#). Com base na configuração da rede e na produtividade dos canais de comunicação, defina o número de Servidores de Administração a serem usados e como eles devem ser distribuídos entre seus escritórios (se você executar uma rede distribuída).

Defina se uma [hierarquia de Servidores de Administração](#) será usada na sua organização. Para fazer isto, você deve avaliar se é possível e conveniente cobrir todos os dispositivos cliente com um único Servidor de Administração ou se é necessário criar uma hierarquia de Servidores de Administração. Você também deveria criar uma hierarquia de Servidores de Administração que seja idêntica à estrutura organizacional da sua organização cuja rede você pretende proteger.

2 Preparação para o uso de certificados personalizados

Se a infraestrutura de chave pública (PKI) da sua organização exige que você use certificados personalizados emitidos por uma autoridade de certificação (CA) específica, prepare esses [certificados](#) e garanta que eles atendam a todos os [requisitos](#).

3 Instalação de um sistema de gerenciamento de banco de dados (DBMS)

[Instale o DBMS](#) que será usado pelo Kaspersky Security Center ou use um existente.

4 Configuração de portas

Assegure-se de que todas as [portas](#) necessárias estão abertas para a interação entre os componentes de acordo com a sua estrutura de segurança selecionada.

Se tiver que fornecer acesso à Internet para o Servidor de Administração, configure as portas e especifique as configurações de conexão, dependendo da configuração da rede.

5 Instalando o Kaspersky Security Center

Selecione um dispositivo Linux que deseja usar como Servidor de Administração, certifique-se de que o dispositivo atende aos [requisitos de hardware e software](#). Depois, [instale o Kaspersky Security Center](#) no dispositivo. A versão do servidor do Agente de Rede será instalada junto com o Servidor de Administração.

6 Instalando o Kaspersky Security Center 14 Web Console e os plugins de gerenciamento da web

Selecione um dispositivo Linux que deseja usar como estação de trabalho do administrador, certifique-se de que o dispositivo atende aos [requisitos de hardware e software](#). Depois, instale o Kaspersky Security Center 14 Web Console no dispositivo. Você pode instalar o Kaspersky Security Center 14 Web Console no mesmo dispositivo onde o Servidor de Administração está instalado ou em outro.

[Baixe o plugin da Web de gerenciamento do Kaspersky Endpoint Security for Linux](#) e instale-o no mesmo dispositivo no qual o Kaspersky Security Center 14 Web Console está instalado.

7 Instalando o Kaspersky Endpoint Security para Linux e Agente de Rede no dispositivo do Servidor de Administração

Por padrão, o aplicativo não considera o dispositivo do Servidor de Administração como um dispositivo gerenciado. Para proteger o Servidor de Administração contra vírus e outras ameaças e para gerenciar o dispositivo, e quaisquer outro dispositivo gerenciado, recomendamos [instalar o Kaspersky Endpoint Security for Linux](#) e o [Agente de Rede para Linux](#) no dispositivo do Servidor de Administração. Nesse caso, o Agente de Rede para Linux é instalado e funciona independentemente da versão do servidor do Agente de Rede que você instalou junto com o Administration Server.

8 Execução da configuração inicial

Quando a instalação de Servidor de Administração estiver concluída, na primeira conexão ao Servidor de Administração o [Assistente de Início Rápido](#) inicia automaticamente. Execute a configuração inicial do Servidor de Administração de acordo com os requisitos existentes. Durante a etapa de configuração inicial, o Assistente usa as configurações padrão para criar as [políticas](#) e [tarefas](#) que são necessárias para implementar a proteção. No entanto, as configurações padrão podem ser menos ótimas para as necessidades da sua organização. Se necessário, você pode [editar as configurações das políticas e tarefas](#).

9 Localização de dispositivos na rede

Realize a detecção de dispositivos manualmente. O Kaspersky Security Center Linux recebe os endereços e os nomes de todos os dispositivos detectados na rede. Você então pode usar o Kaspersky Security Center Linux para instalar aplicativos Kaspersky e software de outros fornecedores nos dispositivos detectados. O Kaspersky Security Center Linux regularmente inicia uma descoberta de dispositivos, o que significa que se alguma nova instância aparecer na rede, ela será detectada automaticamente.

10 Organização de dispositivos em grupos de administração

Em alguns casos, implementar a proteção em dispositivos na rede no modo mais conveniente pode necessitar que você [divida todo o conjunto de dispositivos em grupos de administração](#), considerando a estrutura da organização. Você pode criar [regras para mover para distribuir dispositivos entre grupos](#) ou pode distribuir os dispositivos manualmente. Você pode atribuir tarefas de grupo para grupos de administração, definir o escopo das políticas e atribuir pontos de distribuição.

Assegure-se de que todos os dispositivos gerenciados foram corretamente atribuídos aos grupos de administração apropriados, e que não mais haja dispositivos não atribuídos na rede.

11 Atribuir os pontos de distribuição

Os pontos de distribuição são atribuídos aos grupos de administração automaticamente, mas você pode atribuí-los manualmente, se necessário. Recomendamos que você use pontos de distribuição em redes de larga escala para reduzir a carga no Servidor de Administração, e em redes que têm uma estrutura distribuída para fornecer ao Servidor de Administração o acesso aos dispositivos (ou grupos de dispositivos) comunicado através de canais com baixas taxas de produtividade.

12 Instalar o Agente de Rede e aplicativos de segurança em dispositivos na rede

A implementação da proteção em uma rede corporativa engloba a [instalação do Agente de Rede e de aplicativos de segurança](#) nos dispositivos que foram detectados pelo Servidor de Administração durante a descoberta de dispositivos.

Para instalar os aplicativos remotamente, execute o Assistente de Implementação da Proteção.

Os aplicativos de segurança protegem os dispositivos contra vírus e outros programas que apresentem uma ameaça. O Agente de Rede assegura a comunicação entre o dispositivo e o Servidor de Administração. As configurações do Agente de Rede são definidas automaticamente por padrão.

Antes que você inicie a instalação do Agente de Rede e dos aplicativos de segurança nos dispositivos na rede, assegure-se de que estes dispositivos estejam acessíveis (ligados).

13 Implementação de chaves de licença para dispositivos cliente

Implemente [chaves de licença](#) em dispositivos cliente para ativar aplicativos de segurança gerenciados naqueles dispositivos.

14 Configuração de políticas de aplicativo da Kaspersky

Para aplicar configurações de aplicativo diferentes a dispositivos diferentes, você pode usar gerenciamento de segurança centrado no dispositivo e/ou gerenciamento de segurança centrado no usuário. O gerenciamento de segurança centrado no dispositivo pode ser implementado usando [políticas](#) e [tarefas](#). Você pode aplicar tarefas somente aos dispositivos que atendem a condições específicas. Para definir as condições para filtrar dispositivos, use [seleções de dispositivos](#) e [identificadores](#).

15 Monitorar o status da proteção da rede

Você pode monitorar sua rede usando widgets no [relatório](#), gerar [relatórios](#) a partir de aplicativos da Kaspersky, configurar e visualizar [seleções de eventos](#) recebidos dos aplicativos nos dispositivos gerenciados e visualizar listas de notificações.

Instalação de um sistema de gerenciamento de banco de dados

Instalar o sistema de gerenciamento de banco de dados (DBMS) que será usado pelo Kaspersky Security Center. Você pode selecionar um dos [DBMSs compatíveis](#).

Para obter informações sobre como instalar o DBMS selecionado, consulte a sua documentação.

Se usar o MariaDB, é necessário [definir as configurações recomendadas](#) para um funcionamento ideal do DBMS com o Kaspersky Security Center.

Configurando o servidor MariaDB x64 para trabalhar com o Kaspersky Security Center 14 Linux

Se você usa o servidor MariaDB para o Kaspersky Security Center, ative a compatibilidade para armazenamento InnoDB e MEMORY e as codificações UTF-8 e UCS-2.

Configurações recomendadas para o arquivo my.cnf

Para configurar o arquivo my.cnf:

1. [Abra o arquivo my.cnf](#) em qualquer editor de texto.

2. Insira as seguintes linhas no arquivo my.cnf:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
```



```
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< value >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count = 12800
table_open_cache = 60000
table_open_cache_instances = 4
table_definition_cache = 60000
```

O valor de `innodb_buffer_pool_size` não deve ser inferior a 80% do tamanho esperado do banco de dados KAV.

Recomenda-se usar o valor do parâmetro `innodb_flush_log_at_trx_commit = 0`, pois os valores "1" ou "2" afetam negativamente a velocidade de operação do MariaDB.

Por padrão, os complementos do otimizador `join_cache_incremental`, `join_cache_hashed`, `join_cache_bka` estão ativados. Se esses complementos não estiverem ativados, você deve ativá-los.

Para verificar se os complementos do otimizador estão ativados:

1. No console do cliente MariaDB, execute o comando:

```
SELECT @@optimizer_switch;
```

2. Verifique se a saída contém as seguintes linhas:

```
join_cache_incremental=on
join_cache_hashed=on
join_cache_bka=on
```

Se essas linhas estiverem presentes e com os valores ativados, os complementos do otimizador serão ativados.

Se estas linhas estiverem ausentes ou tiverem valores desativados, você precisa fazer o seguinte:

a. Abra o arquivo `my.cnf` em um editor de texto.

b. Adicione as seguintes linhas ao arquivo `my.cnf`:

```
optimizer_switch='join_cache_incremental=on'
optimizer_switch='join_cache_hashed=on'
optimizer_switch='join_cache_bka=on'
```

Os complementos `join_cache_incremental`, `join_cache_hash`, e `join_cache_bka` estão ativados.

Instalando o Kaspersky Security Center

Este procedimento descreve como instalar o Kaspersky Security Center.

Antes da instalação:

- Instale um [sistema de gerenciamento de banco de dados](#).
- Certifique-se de que o dispositivo no qual você quer instalar o Kaspersky Security Center está executando em uma das [distribuições Linux compatíveis](#).

Use o arquivo de instalação `ksc64-[version_number]-amd64.deb` or `ksc64-[version_number].x86_64.rpm`, que corresponde à distribuição Linux instalada no seu dispositivo. Para receber o arquivo de instalação, baixe-o do site da Kaspersky.

Para instalar o Kaspersky Security Center:

1. Na linha de comando, execute os comandos fornecidos nesta instrução em uma conta com privilégios de acesso a raiz.
2. Crie um grupo 'kladmins' e uma conta 'KSC' sem privilégios. A conta deve ser de um membro do grupo kladmins. Para fazer isso, execute os seguintes comandos em sequência:

```
# adduser ksc
# groupadd kladmins
# gpasswd -a ksc kladmins
# usermod -g kladmins ksc
```
3. Execute o Kaspersky Security Center. Dependendo da sua distribuição Linux, execute um dos seguintes comandos:
 - `# apt install /<caminho>/ksc64-[version_number]-amd64.deb`
 - `# yum install /<caminho>/ksc64-[version_number].x86_64.rpm -y`
4. Execute a configuração do Kaspersky Security Center:

```
# /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```
5. Leia o [Contrato de Licença do Usuário Final](#) (EULA) e a Política de Privacidade. O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite os seguintes valores:
 - a. Digite `y` (sim), se você entende e aceita integralmente os termos do EULA. Digite `n` (não) se você não aceita os termos do EULA. Para usar o Kaspersky Security Center, você deve aceitar os termos do EULA.
 - b. Digite `y` (sim) se você entendeu e aceita os termos da Política de Privacidade e se você concorda que seus dados serão tratados e transmitidos (incluindo a países terceiros), conforme descrito na Política de Privacidade. Digite `n` (não) se você não aceita os termos da Política de Privacidade. Para usar o Kaspersky Security Center, você deve aceitar os termos da Política de Privacidade.
6. Quando for solicitado, digite as seguintes configurações:
 - a. Digite o nome DNS do Servidor de Administração ou o endereço IP estático.
 - b. Digite o número da porta do Servidor de Administração. Por padrão, a porta 14000 é usada.
 - c. Digite o número da porta SSL do Servidor de Administração. Por padrão, a porta 13000 é usada.
 - d. Avalie o número aproximado de dispositivos que você deseja gerenciar:
 - Se você tem de 1 a 100 dispositivos em rede, digite 1.
 - Se você tem de 101 a 1000 dispositivos em rede, digite 2.
 - Se você tem mais de 1000 dispositivos em rede, digite 3.
 - e. Digite o nome do grupo de segurança para serviços. Por padrão, é usado o grupo 'kladmins'.

- f. Digite o nome da conta e inicie o serviço do Servidor de Administração. A conta deve ser de um membro do grupo de segurança digitado. Por padrão, é usada a conta 'KSC'.
- g. Digite o nome da conta para iniciar outros serviços. A conta deve ser de um membro do grupo de segurança digitado. Por padrão, é usada a conta 'KSC'.
- h. Digite o endereço IP do dispositivo no qual o banco de dados está instalado.
- i. Digite o número da porta do banco de dados. Esta porta é usada para comunicação com o Servidor de Administração. Por padrão, a porta 3306 é usada.
- j. Digite o nome do banco de dados.
- k. Digite o login da conta raiz do banco de dados usada para acessar o banco de dados.
- l. Digite a senha da conta raiz do banco de dados usada para acessar o banco de dados.
Aguarde que os serviços sejam adicionados e inicializados automaticamente:
- `klagent_srv`
 - `kladminserver_srv`
 - `klactprx_srv`
 - `klwebsrv_srv`
- m. Crie uma conta que agirá como um administrador do Servidor de Administração. Digite o nome de usuário e senha.
- A senha deve estar em conformidade com as seguintes regras:
- A senha de usuário não pode ter menos de 8 nem mais de 16 caracteres.
 - A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
 - Letras maiúsculas (A-Z)
 - Letras minúsculas (a-z)
 - Números (0-9)
 - Caracteres especiais (@ # \$ % ^ & * - _ ! + = [] { } | : ' . ? / \ ` ~ " () ;)

O usuário é adicionado e o Kaspersky Security Center é instalado.

Verificação de serviço

Use os comandos a seguir para verificar se o serviço está sendo executando ou não:

- `# systemctl status klagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`

- # systemctl status klwebsrv_srv.service

Instalar o Kaspersky Security Center 14 Web Console

Esta seção descreve como instalar o Kaspersky Security Center 14 Web Console Server (também mencionado como Kaspersky Security Center 14 Web Console) em dispositivos que executam o sistema operacional Linux. Antes da instalação, você deve instalar um [sistema de gerenciamento de banco de dados](#) e o Servidor de Administração do [Kaspersky Security Center](#).

Use um dos seguintes arquivos de instalação que corresponda à distribuição Linux instalada em seu dispositivo:

- Para Debian, ksc-web-console-[build_number].x86_64.deb
- Para sistemas operacionais baseados em RPM, ksc-web-console-[build_number].x86_64.rpm
- Para Alt 8 SP, ksc-web-console-[build_number]-alt8p.x86_64.rpm

Para receber o arquivo de instalação, baixe-o do site da Kaspersky.

Para instalar o Kaspersky Security Center 14 Web Console:

1. Certifique-se de que o dispositivo no qual você quer instalar o Kaspersky Security Center 14 Web Console está executando uma das distribuições Linux compatíveis.
2. Leia o Contrato de Licença do Usuário Final (EULA) no pacote de instalação (arquivo /var/opt/kaspersky/ksc-web-console/license-<XX>.txt, em que <XX> é um código de idioma). Se você não aceitar os termos do Contrato de Licença, não instale o aplicativo.
3. Crie um [arquivo de resposta](#) que contenha parâmetros para conectar o Kaspersky Security Center 14 Web Console ao Servidor de Administração. Nomeie esse arquivo ksc-web-console-setup.json e coloque-o no seguinte diretório: /etc/ksc-web-console-setup.json.

Exemplo de um arquivo de resposta que contém o conjunto mínimo de parâmetros e o endereço e a porta padrão:

```
{
  "address": "127.0.0.1",
  "port": 8080,
  "trusted":
  "127.0.0.1|13299|/var/opt/kaspersky/klagent_srv/1093/cert/klserver.cer|KSC
  Server",
  "acceptEula": true
}
```

Ao instalar o Kaspersky Security Center 14 Web Console no sistema operacional Linux ALT, você deve especificar um número de porta diferente de 8080, pois essa porta é usada pelo sistema operacional.

Kaspersky Security Center 14 Web Console não pode ser atualizado usando o mesmo arquivo de instalação .rpm. Se você deseja alterar as configurações em um arquivo de resposta e usar esse arquivo para reinstalar o aplicativo, primeiro remova o aplicativo e, em seguida, instale-o novamente com o novo arquivo de resposta.

4. Em uma conta com privilégios de raiz, use a linha de comando para executar o arquivo de configuração com a extensão .deb ou .rpm, dependendo da sua distribuição Linux.

- Para instalar ou atualizar o Kaspersky Security Center 14 Web Console a partir de um arquivo .deb, execute o seguinte comando:

```
$ sudo dpkg -i ksc-web-console-[ build_number ].x86_64.deb
```

- Para instalar o Kaspersky Security Center 14 Web Console a partir de um arquivo .rpm, execute os seguintes comandos:

```
$ sudo rpm -ivh --nodeps ksc-web-console-[ build_number ].x86_64.rpm
```

ou

```
$ sudo alien -i ksc-web-console-[ build_number ].x86_64.rpm
```

- Para atualizar de uma versão anterior do Kaspersky Security Center Web Console, execute um dos seguintes comandos:

- Para os dispositivos que executam sistema operacional baseado em RPM:

```
$ sudo rpm -Uvh --nodeps --force ksc-web-console-[ build_number ].x86_64.rpm
```

- Para os dispositivos com sistema operacional baseado em Debian:

```
$ sudo dpkg -i ksc-web-console-[ build_number ].x86_64.deb
```

Essa ação inicia a descompactação do arquivo de configuração. Espere até que a instalação seja concluída. Kaspersky Security Center 14 Web Console está instalado no seguinte diretório: /var/opt/kaspersky/ksc-web-console.

5. Reinicie os serviços do Kaspersky Security Center 14 Web Console executando o seguinte comando:

```
$ sudo systemctl restart KSC*
```

Quando a instalação estiver concluída, você poderá usar o navegador para [abrir e fazer login no Kaspersky Security Center 14 Web Console](#).

Parâmetros de instalação do Kaspersky Security Center 14 Web Console

Para [instalar o Kaspersky Security Center 14 Web Console Server em dispositivos que executam o Linux](#), você deve criar um arquivo de resposta, um arquivo .json que contém parâmetros para conectar o Kaspersky Security Center 14 Web Console ao Servidor de Administração.

Veja o exemplo de um arquivo de resposta que contém o conjunto mínimo de parâmetros e o endereço e a porta padrão:

```
{
  "address": "127.0.0.1",
  "port": 8080,
  "defaultLangId": 1049,
  "enableLog": false,
  "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
  "webConsoleAccount": "Group1:User1",
  "managementServiceAccount": "Group1:User2",
  "serviceWebConsoleAccount": "Group1:User3",
  "pluginAccount": "Group1:User4",
```

```
"messageQueueAccount": "Group1:User5"
}
```

Ao instalar o Kaspersky Security Center 14 Web Console no sistema operacional Linux ALT, é necessário especificar um número de porta diferente de 8080, pois essa porta é usada pelo sistema operacional.

A tabela abaixo descreve os parâmetros que podem ser especificados em um arquivo de resposta.

Parâmetros para instalar o Kaspersky Security Center 14 Web Console em dispositivos que executam o Linux

Parâmetro	Descrição	Valores dispon
address	Endereço do Kaspersky Security Center 14 Web Console Server (necessário).	Valor da sequência de caracteres.
port	Número da porta que o Kaspersky Security Center 14 Web Console Server usará para se conectar ao Servidor de Administração (necessário).	Valor numérico.
defaultLangId	Idioma da interface do usuário (por padrão, 1033).	<p>Código numérico do idioma:</p> <ul style="list-style-type: none"> • Alemão: 1031 • Inglês: 1033 • Espanhol: 3082 • Espanhol (México): 2058 • Francês: 1036 • Japonês: 1041 • Cazaque: 1087 • Polonês: 1045 • Português (Brasil): 1046 • Russo: 1049 • Turco: 1055 • Chinês simplificado: 4 • Chinês tradicional: 31748 <p>Se nenhum valor for especificado, o idioma</p>
enableLog	Se ativar o registro da atividade do Kaspersky Security Center 14 Web Console.	<p>Valor booleano:</p> <ul style="list-style-type: none"> • true — o registro é ativado (selecione • false — o registro é desativado.

trusted	<p>Lista de Servidores de Administração de confiança permitidos a conectarem-se ao Kaspersky Security Center 14 Web Console. Cada Servidor de Administração deve ser definido com os seguintes parâmetros:</p> <ul style="list-style-type: none"> • Endereço do Servidor de Administração • Porta OpenAPI que é usada pelo Kaspersky Security Center 14 Web Console para se conectar ao Servidor de Administração (por padrão, 13299) • Caminho para o certificado do Servidor de Administração • Nome do Servidor de Administração que será exibido na janela de login <p>Os parâmetros são separados por barras verticais. Se vários Servidores de Administração forem especificados, separe-os por duas barras verticais (pipes).</p>	<p>Valor da sequência de caracteres no seguinte formato: <code>server address port certificate</code></p> <p>Exemplo:</p> <pre>"X.X.X.X 13299 /cert/server-1.cer Y.Y.Y.Y 13299 /cert/server-2.cer"</pre>
acceptEula	<p>Se você aceita ou não os termos do Contrato de Licença do Usuário Final (EULA). O arquivo que contém os termos do EULA é baixado junto com o arquivo de instalação.</p>	<p>Valor booleano:</p> <ul style="list-style-type: none"> • <code>true</code>—Eu li entendo e aceito por completo os termos do Contrato de Licença do Usuário Final. • <code>false</code>—Eu não aceito os termos do Contrato de Licença do Usuário Final (selecionado por padrão).
certDomain	<p>Se você quiser gerar um novo certificado, use este parâmetro para especificar o nome de domínio para o qual um novo certificado deve ser gerado.</p>	<p>Valor da sequência de caracteres.</p>
certPath	<p>Se você quiser usar um certificado existente, use este parâmetro para especificar o caminho até o arquivo de certificado.</p>	<p>Valor da sequência de caracteres.</p> <p>Especifique o caminho <code>" /var/opt/kaspersky/klnagent_srv "</code> para utilizar o certificado existente. Para utilizar um certificado diferente, especifique o caminho onde o certificado está armazenado.</p>
keyPath	<p>Se você quiser usar um certificado existente, use este parâmetro para especificar o caminho até o arquivo de chave.</p>	<p>Valor da sequência de caracteres.</p>
webConsoleAccount	<p>Nome da conta sob a qual o serviço KSCWebConsole é executado.</p>	<p>Valor da sequência de caracteres no seguinte formato: <code>grupo:nome do usuário</code>.</p> <p>Exemplo: <code>"Group1:User1"</code>.</p>

		Se nenhum valor for especificado, o instalador do Kaspersky Security Center 14 Web Console criará uma nova conta de usuário com o nome <code>user_management_%uid%</code> .
<code>managementServiceAccount</code>	Nome da conta privilegiada sob a qual o serviço KSCWebConsoleManagement é executado.	Valor da sequência de caracteres no seguinte formato: <code>grupo:nome do usuário</code> . Exemplo: "Group1:User1". Se nenhum valor for especificado, o instalador do Kaspersky Security Center 14 Web Console criará uma nova conta de usuário com o nome <code>user_nodejs_%uid%</code> .
<code>serviceWebConsoleAccount</code>	Nome da conta sob a qual o serviço KSCSvcWebConsole é executado.	Valor da sequência de caracteres no seguinte formato: <code>grupo:nome do usuário</code> . Exemplo: "Group1:User1". Se nenhum valor for especificado, o instalador do Kaspersky Security Center 14 Web Console criará uma nova conta de usuário com o nome <code>user_svc_nodejs_%uid%</code> .
<code>pluginAccount</code>	Nome da conta sob a qual o serviço KSCWebConsolePlugin é executado.	Valor da sequência de caracteres no seguinte formato: <code>grupo:nome do usuário</code> . Exemplo: "Group1:User1". Se nenhum valor for especificado, o instalador do Kaspersky Security Center 14 Web Console criará uma nova conta de usuário com o nome <code>user_web_plugin_%uid%</code> .
<code>messageQueueAccount</code>	Nome da conta sob a qual o serviço KSCWebConsoleMessageQueue é executado.	Valor da sequência de caracteres no seguinte formato: <code>grupo:nome do usuário</code> . Exemplo: "Group1:User1". Se nenhum valor for especificado, o instalador do Kaspersky Security Center 14 Web Console criará uma nova conta de usuário com o nome <code>user_message_queue_%uid%</code> .

Se você especificar os parâmetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` ou `messageQueueAccount`, certifique-se de que as contas de usuário personalizadas pertencem ao mesmo grupo de segurança. Se esses parâmetros não forem especificados, o instalador do Kaspersky Security Center 14 Web Console criará um grupo de segurança padrão e, em seguida, criará contas de usuário com nomes padrão nesse grupo.

Contas para trabalhar com o DBMS

A tabela a seguir fornece informações sobre as propriedades das contas selecionadas para trabalhar com o DBMS MariaDB.

O *DBMS local* é um DBMS instalado no mesmo dispositivo que o do Servidor de Administração. O *DBMS remoto* é um DBMS instalado em um dispositivo diferente.

Conceda todos os direitos necessários para a conta do Servidor de Administração antes que você inicie o serviço do Servidor de Administração.

DBMS: MariaDB

Localização do DBMS	Local ou remoto.	Local ou remoto.

Quem cria o banco de dados KAV	O instalador (automaticamente).	Administrador (manualmente).
Conta sob a qual o Instalador está sendo executado	Local ou domínio, com direitos de administrador local.	Local ou domínio, com direitos de administrador local.
Conta de serviço do Servidor de Administração	Local ou domínio.	Local ou domínio.
Direitos da conta interna do DBMS usada pelo instalador e pelo serviço do Servidor de Administração para acessar o DBMS	O acesso root é necessário.	CONCEDER TODOS para o banco de dados KAV, e SELECIONAR, EXIBIR VISUALIZAÇÃO, PROCESSO para as tabelas do sistema.

Implementação do cluster de failover da Kaspersky

Esta seção contém informações gerais sobre o cluster de failover da Kaspersky e instruções sobre a preparação e implementação do cluster de failover da Kaspersky em sua rede.

Cenário: implantando um cluster de failover Kaspersky

Um cluster de failover da Kaspersky garante a alta disponibilidade do Kaspersky Security Center e minimiza o tempo de inatividade do Servidor de Administração, em caso de falha. O cluster de failover é baseado em duas instâncias idênticas do Kaspersky Security Center, instaladas em dois computadores. Uma das instâncias funciona como o nó ativo e a outra, como o nó passivo. O nó ativo gerencia a proteção dos dispositivos clientes, enquanto o passivo está preparado para assumir todas as funções do nó ativo caso o nó ativo falhe. Quando ocorre uma falha, o nó passivo torna-se ativo e o nó ativo torna-se passivo.

Pré-requisitos

Você possui hardware que atende aos [requisitos](#) para o cluster de failover.

A implementação dos aplicativos da Kaspersky é feita em fases:

1 Como criar uma conta para os serviços do Kaspersky Security Center

Crie uma nova conta de usuário de domínio ou selecione uma existente na qual os serviços do Kaspersky Security Center serão executados. Adicione a conta selecionada no grupo de administradores locais em cada um dos nós e no servidor de arquivos.

2 Preparação do servidor de arquivos

Prepare o servidor de arquivos para funcionar como um componente do cluster de failover do Kaspersky. Certifique-se de que o servidor de arquivos atenda aos requisitos de hardware e software, crie duas pastas compartilhadas para os dados do Kaspersky Security Center e configure as permissões para acessar as pastas compartilhadas.

Instruções: [Como preparar um servidor de arquivos para o cluster de failover da Kaspersky](#).

3 Preparação de nós ativos e passivos

Prepare dois computadores com hardware e software idênticos para funcionarem como nós ativos e passivos.

Instruções: [Como preparar nós para o cluster de failover da Kaspersky](#).

4 Instalação do sistema de gerenciamento de banco de dados (DBMS)

Você tem duas opções:

- Se quiser usar o MariaDB Galera Cluster, não é necessário um computador dedicado para DBMS. Instale o MariaDB Galera Cluster em cada um dos nós.
- Se quiser usar qualquer outro [DBMS compatível](#), instale o DBMS selecionado em um computador dedicado.

5 Instalação do Kaspersky Security Center

Instale o Kaspersky Security Center no modo de cluster de failover em ambos os nós. Você deve primeiramente instalar o Kaspersky Security Center no nó ativo e depois instalá-lo no passivo.

6 Como testar o cluster de failover

Verifique se você configurou o cluster de failover corretamente e se ele funciona corretamente. Por exemplo, você pode interromper um dos serviços do Kaspersky Security Center no nó ativo: kladminserver, klnagent, ksnproxy, klactprx ou klwebsrv. Após o serviço ser interrompido, o gerenciamento de proteção deve ser alternado automaticamente para o nó passivo.

Resultados

O cluster de failover do Kaspersky é implementado. Conheça os [eventos que levam à alternância entre os nós ativos e passivos](#).

Sobre o cluster de failover da Kaspersky

Um cluster de failover da Kaspersky garante a alta disponibilidade do Kaspersky Security Center e minimiza o tempo de inatividade do Servidor de Administração, em caso de falha. O cluster de failover é baseado em duas instâncias idênticas do Kaspersky Security Center, instaladas em dois computadores. Uma das instâncias funciona como o nó ativo e a outra, como o nó passivo. O nó ativo gerencia a proteção dos dispositivos clientes, enquanto o passivo está preparado para assumir todas as funções do nó ativo caso o nó ativo falhe. Quando ocorre uma falha, o nó passivo torna-se ativo e o nó ativo torna-se passivo.

Em um cluster de failover da Kaspersky, todos os serviços do Kaspersky Security Center são gerenciados automaticamente. Não tente reiniciar os serviços manualmente.

Requisitos de hardware e software

Para implementar um cluster de failover da Kaspersky, você deve ter o seguinte hardware:

- Dois computadores com hardware e software idênticos. Esses computadores atuarão como nós ativos e passivos.
- Um servidor de arquivos executando Linux com o sistema de arquivos EXT4. Você deve fornecer um computador dedicado que funcionará como um servidor de arquivos.

Certifique-se de ter alta largura de banda de rede entre o servidor de arquivos e os nós ativos e passivos.

- Um computador com sistema de gerenciamento de banco de dados (DBMS). Se você usa o MariaDB Galera Cluster como um DBMS, não é necessário um computador dedicado para essa finalidade.

Condições de alternância

O cluster de failover alterna o gerenciamento de proteção dos dispositivos clientes do nó ativo para o nó passivo se qualquer um dos seguintes eventos ocorrer no nó ativo:

- O nó ativo foi interrompido devido a uma falha de software ou hardware.
- O nó ativo foi temporariamente interrompido por atividades de [manutenção](#).
- Pelo menos um dos serviços (ou processos) do Kaspersky Security Center falhou ou foi encerrado deliberadamente pelo usuário. Os serviços do Kaspersky Security Center são os seguintes: kladminserver, klnagent, klactprx e klwebsrv.
- A conexão de rede entre o nó ativo e o armazenamento no servidor de arquivos foi interrompida ou encerrada.

Preparando um servidor de arquivos para um cluster de failover da Kaspersky

Um servidor de arquivos funciona como um componente necessário de um [cluster de failover da Kaspersky](#).

Para preparar um servidor de arquivos:

1. Certifique-se de que o servidor de arquivos atenda aos [requisitos de hardware e software](#).
2. Instalar e configurar um servidor NFS:
 - O acesso ao servidor de arquivos deve ser ativado para os dois nós nas configurações do servidor NFS.
 - O protocolo NFS deve ter a versão 4.0 ou 4.1.
 - Requisitos mínimos para o kernel do Linux:
 - 3.19.0-25, if you use NFS 4.0
 - 4.4.0-176, if you use NFS 4.1
3. No servidor de arquivos, crie duas pastas e compartilhe-as usando o NFS. Uma delas é usada para manter informações sobre o estado do cluster de failover. A outra é usada para armazenar os dados e configurações do Kaspersky Security Center. Você especificará caminhos para as pastas compartilhadas ao configurar a [instalação do Kaspersky Security Center](#).

Execute os seguintes comandos:

```
sudo yum install nfs-utils
sudo mkdir -p /mnt/KlFocStateShare
sudo mkdir -p /mnt/KlFocDataShare_klfoc
sudo chown ksc:kladmins /mnt/KlFocStateShare
sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
sudo sh -c "echo /mnt/KlFocStateShare *\ (rw, sync, no_subtree_check, no_root_squash\ ) >> /etc/exports"
sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\ (rw, sync, no_subtree_check, no_root_squash\ ) >> /etc/exports"
sudo cat /etc/exports
sudo exportfs -a
```

```
sudo systemctl start rpcbind
sudo service nfs start
```

Ative a inicialização automática executando o seguinte comando:

```
sudo systemctl enable rpcbind
```

4. Reinicie o servidor de arquivos.

O servidor de arquivos está preparado. Para implantar o cluster de failover da Kaspersky, siga as instruções adicionais neste [cenário](#).

Preparando nós para um cluster de failover da Kaspersky

Prepare dois computadores para trabalhar como nós ativos e passivos do [cluster de failover da Kaspersky](#).

Para preparar nós para um cluster de failover da Kaspersky:

1. Certifique-se de ter dois computadores que atendam aos [requisitos de hardware e software](#). Esses computadores atuarão como nós ativos e passivos do cluster de failover.

2. Para fazer os nós funcionarem como clientes NFS, instale o pacote nfs-utils em cada nó.

Execute o seguinte comando:

```
sudo yum install nfs-utils
```

3. Crie pontos de montagem executando os seguintes comandos:

```
sudo mkdir -p /mnt/K1FocStateShare
sudo mkdir -p /mnt/K1FocDataShare_k1foc
```

4. Verifique se as pastas compartilhadas podem ser montadas com êxito. [etapa opcional]

Execute os seguintes comandos:

```
sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {servidor}:{caminho
para a pasta K1FocStateShare} /mnt/K1FocStateShare
sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {servidor}:
{caminho para a pasta K1FocDataShare_k1foc} /mnt/K1FocDataShare_k1foc
```

Aqui, {servidor}:{caminho para a pasta K1FocStateShare} e {servidor}:{caminho para a pasta K1FocDataShare_k1foc} são os caminhos de rede para as pastas compartilhadas no servidor de arquivos.

Depois que as pastas compartilhadas forem montadas com sucesso, desmonte-as executando os seguintes comandos:

```
sudo umount /mnt/K1FocStateShare
sudo umount /mnt/K1FocDataShare_k1foc
```

5. Corresponda os pontos de montagem e as pastas compartilhadas:

```
sudo vi /etc/fstab
{servidor}:{caminho para a pasta K1FocStateShare} /mnt/K1FocStateShare nfs
vers=4,nolock,local_lock=none,auto,user,rw 0 0
{servidor}:{caminho para a pasta K1FocDataShare_k1foc} /mnt/K1FocDataShare_k1foc nfs
vers=4,nolock,local_lock=none,noauto,user,rw 0 0
```

Aqui, {servidor}:{caminho para a pasta K1FocStateShare} e {servidor}:{caminho para a pasta K1FocDataShare_k1foc} são os caminhos de rede para as pastas compartilhadas no servidor de arquivos.

6. Reinicie os dois nós.

7. Monte as pastas compartilhadas executando os seguintes comandos:

```
mount /mnt/K1FocStateShare
mount /mnt/K1FocDataShare_k1foc
```

8. Certifique-se de que as permissões para acessar as pastas compartilhadas pertençam a ksc:kladmins.

Execute o seguinte comando:

```
sudo ls -la /mnt/
```

9. Execute uma das seguintes ações:

- Em cada um dos nós, crie um adaptador de rede virtual. Por exemplo, execute os seguintes comandos:

a. Descubra os nomes de interface executando o seguinte comando:

```
ifconfig
```

b. Execute o seguinte script (daqui em diante, os nomes das interfaces são fornecidos como exemplos):

```
#!/bin/bash
PHYSICAL_IFACE=ens160
VIRTUAL_IFACE=macvlan1
ip link del $VIRTUAL_IFACE > /dev/null 2>&1
ip link add link $PHYSICAL_IFACE $VIRTUAL_IFACE type macvlan
if [ "$?" -ne "0" ]; then
    echo ERROR adding new virtual adapter $VIRTUAL_IFACE!
    exit $?
fi
ip link set $VIRTUAL_IFACE down
if [ "$?" -ne "0" ]; then
    echo ERROR disabling virtual adapter $VIRTUAL_IFACE!
    exit $?
fi
```

c. Execute o seguinte comando:

```
ip addr add {endereço IP do adaptador de rede virtual } dev {nome do
adaptador de rede virtual}
```

O endereço IP deve estar vazio quando você criar o adaptador de rede virtual. Os adaptadores de rede virtual em ambos os nós devem ter o mesmo endereço IP.

d. Verifique se o adaptador de rede virtual foi criado com êxito.

Execute os seguintes comandos:

```
ip link set macvlan1 up
ifconfig
```

e. Desative o adaptador de rede virtual executando o seguinte comando:

```
ip link set macvlan1 down
```

- Use um balanceador de carga de terceiros. Por exemplo, você pode usar um servidor nginx. Nesse caso, faça o seguinte:

a. Forneça um computador dedicado baseado em Linux com nginx instalado.

b. Configure o balanceamento de carga. Defina o nó ativo como o servidor principal e o nó passivo como um servidor de backup.

c. No servidor nginx, abra todas as portas do Servidor de Administração: TCP 13000, UDP 13000, TCP 13291, TCP 13299, TCP 17000.

Os nós estão preparados. Para implantar um cluster de failover da Kaspersky, siga as instruções adicionais do [cenário](#).

Instalando o Kaspersky Security Center nos nós do cluster de failover da Kaspersky

Este procedimento descreve como instalar o Kaspersky Security Center nos nós do [cluster de failover da Kaspersky](#). O Kaspersky Security Center é instalado em ambos os nós do cluster de failover da Kaspersky separadamente. Primeiro, você instala o aplicativo no nó ativo e, em seguida, no passivo. Ao instalar, você escolhe qual nó ficará ativo e qual será passivo.

Use o arquivo de instalação `ksc64-[version_number]-amd64.deb` or `ksc64-[version_number].x86_64.rpm`, que corresponde à distribuição Linux instalada no seu dispositivo. Para receber o arquivo de instalação, baixe-o do site da Kaspersky.

Apenas um usuário do grupo de domínio KLAAdmins pode instalar o Kaspersky Security Center em cada nó.

Instalação no nó primário (ativo)

Para instalar o Kaspersky Security Center no nó primário:

1. Certifique-se de que o dispositivo no qual você quer instalar o Kaspersky Security Center está executando em uma das [distribuições Linux compatíveis](#).
2. Na linha de comando, execute os comandos fornecidos nesta instrução em uma conta com privilégios de acesso a raiz.
3. Execute o Kaspersky Security Center. Dependendo da sua distribuição Linux, execute um dos seguintes comandos:
 - `sudo apt install /<caminho>/ksc64-[version_number]-amd64.deb`
 - `sudo yum install /<caminho>/ksc64-[version_number].x86_64.rpm -y`
4. Execute a configuração do Kaspersky Security Center:

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```
5. Leia o [Contrato de Licença do Usuário Final](#) (EULA) e a Política de Privacidade. O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite os seguintes valores:
 - a. Digite `y` (sim), se você entende e aceita integralmente os termos do EULA. Digite `n` (não) se você não aceita os termos do EULA. Para usar o Kaspersky Security Center, você deve aceitar os termos do EULA.
 - b. Digite `y` (sim) se você entendeu e aceita os termos da Política de Privacidade e se você concorda que seus dados serão tratados e transmitidos (incluindo a países terceiros), conforme descrito na Política de Privacidade. Digite `n` (não) se você não aceita os termos da Política de Privacidade. Para usar o Kaspersky Security Center, você deve aceitar os termos da Política de Privacidade.
6. Selecione o **Nó de cluster primário** como um modo de instalação do Servidor de Administração.

7. Quando for solicitado, digite as seguintes configurações:

- a. Insira o caminho local para o ponto de montagem do compartilhamento de estado.
- b. Insira o caminho local para o ponto de montagem do compartilhamento de dados.
- c. Escolha o modo de conectividade do cluster de failover: por meio de um adaptador de rede virtual ou de um balanceador de carga externo.
- d. Se um adaptador de rede virtual for usado, insira o nome dele.
- e. Quando for solicitada a inserção do nome DNS do Servidor de Administração ou do endereço IP estático, digite o endereço IP do adaptador de rede virtual ou o endereço IP do balanceador de carga externo.
- f. Digite o número da porta do Servidor de Administração. Por padrão, a porta 14000 é usada.
- g. Digite o número da porta SSL do Servidor de Administração. Por padrão, a porta 13000 é usada.
- h. Avalie o número aproximado de dispositivos que você deseja gerenciar:
 - Se você tem de 1 a 100 dispositivos em rede, digite 1.
 - Se você tem de 101 a 1000 dispositivos em rede, digite 2.
 - Se você tem mais de 1000 dispositivos em rede, digite 3.
- i. Digite o nome do grupo de segurança para serviços. Por padrão, é usado o grupo 'kldadmins'.
- j. Digite o nome da conta e inicie o serviço do Servidor de Administração. A conta deve ser de um membro do grupo de segurança digitado. Por padrão, é usada a conta 'KSC'.
- k. Digite o nome da conta para iniciar outros serviços. A conta deve ser de um membro do grupo de segurança digitado. Por padrão, é usada a conta 'KSC'.
- l. Digite o endereço IP do dispositivo no qual o banco de dados está instalado.
- m. Digite o número da porta do banco de dados. Esta porta é usada para comunicação com o Servidor de Administração. Por padrão, a porta 3306 é usada.
- n. Digite o nome do banco de dados.
- o. Digite o login da conta raiz do banco de dados usada para acessar o banco de dados.
- p. Digite a senha da conta raiz do banco de dados usada para acessar o banco de dados.
Aguarde que os serviços sejam adicionados e inicializados automaticamente:
 - klnagent_srv
 - kladminserver_srv
 - klactprx_srv
 - klwebsrv_srv
- q. Crie uma conta que agirá como um administrador do Servidor de Administração. Digite o nome de usuário e senha. A senha de usuário não pode ter menos de 8 nem mais de 16 caracteres.

O usuário é adicionado e o Kaspersky Security Center é instalado no nó primário.

Instalação no nó secundário (passivo)

Para instalar o Kaspersky Security Center no nó secundário:

1. Certifique-se de que o dispositivo no qual você quer instalar o Kaspersky Security Center está executando em uma das [distribuições Linux compatíveis](#).
2. Na linha de comando, execute os comandos fornecidos nesta instrução em uma conta com privilégios de acesso a raiz.
3. Execute o Kaspersky Security Center. Dependendo da sua distribuição Linux, execute um dos seguintes comandos:
 - `sudo apt install /<caminho>/ksc64-[version_number]_amd64.deb`
 - `sudo yum install /<caminho>/ksc64-[version_number].x86_64.rpm -y`
4. Execute a configuração do Kaspersky Security Center:
`sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`
5. Leia o [Contrato de Licença do Usuário Final](#) (EULA) e a Política de Privacidade. O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite os seguintes valores:
 - a. Digite y (sim), se você entende e aceita integralmente os termos do EULA. Digite n (não) se você não aceita os termos do EULA. Para usar o Kaspersky Security Center, você deve aceitar os termos do EULA.
 - b. Digite y (sim) se você entendeu e aceita os termos da Política de Privacidade e se você concorda que seus dados serão tratados e transmitidos (incluindo a países terceiros), conforme descrito na Política de Privacidade. Digite n (não) se você não aceita os termos da Política de Privacidade. Para usar o Kaspersky Security Center, você deve aceitar os termos da Política de Privacidade.
6. Selecione o **Nó de cluster secundário** como um modo de instalação do Servidor de Administração.
7. Quando for solicitado, insira o caminho local para o ponto de montagem do compartilhamento de estado.

O Kaspersky Security Center é instalado no nó secundário.

Verificação de serviço

Use os comandos a seguir para verificar se o serviço está sendo executando ou não:

- `systemctl status klagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

Agora, você pode testar o cluster de failover da Kaspersky para verificar se o configurou corretamente e se o cluster funciona corretamente.

Iniciando e interrompendo nós de cluster manualmente

Pode ser necessário interromper todo o cluster de failover do Kaspersky ou desvincular temporariamente um dos nós do cluster para manutenção. Nesse caso, siga as instruções nesta seção. Não tente iniciar ou interromper os serviços ou processos relacionados ao cluster de failover usando qualquer outro meio. Isso pode causar a perda de dados.

Iniciando e interrompendo todo o cluster de failover para manutenção

Para iniciar ou interromper todo o cluster de failover:

1. No nó ativo, acesse `/opt/kaspersky/ksc64/sbin`.
2. Abra a linha de comando e execute um dos seguintes comandos:
 - Para interromper o cluster, execute: `klfoc -stopcluster --stp klfoc`
 - Para iniciar o cluster, execute: `klfoc -startcluster --stp klfoc`

O cluster de failover é iniciado ou interrompido, de acordo com o comando executado.

Mantendo um dos nós

Para manter um dos nós:

1. No nó ativo, interrompa o cluster de failover usando o comando `klfoc -stopcluster --stp klfoc`.
2. No nó que deseja manter, acesse `/opt/kaspersky/ksc64/sbin`.
3. Abra a linha de comando e desvincule o nó do cluster executando o comando `detach_node.sh`.
4. No nó ativo, inicie o cluster de failover usando o comando `klfoc -startcluster --stp klfoc`.
5. Execute as atividades de manutenção.
6. No nó ativo, interrompa o cluster de failover usando o comando `klfoc -stopcluster --stp klfoc`.
7. No nó que foi mantido, acesse `/opt/kaspersky/ksc64/sbin`.
8. Abra a linha de comando e vincule o nó ao cluster executando o comando `attach_node.sh`.
9. No nó ativo, inicie o cluster de failover usando o comando `klfoc -startcluster --stp klfoc`.

O nó é mantido e conectado ao cluster de failover.

Certificados para trabalhar com o Kaspersky Security Center

A seção contém informações sobre certificados do Kaspersky Security Center e sobre como emitir substituir certificados para o Kaspersky Security Center 14 Web Console e como renovar um certificado para o Servidor de Administração se o Servidor interagir com o Kaspersky Security Center 14 Web Console.

Sobre os certificados do Kaspersky Security Center

O Kaspersky Security Center usa os seguintes tipos de certificados para permitir uma interação segura entre os componentes do aplicativo:

- Certificado do Servidor de Administração
- Certificado do servidor da Web
- Certificado do Kaspersky Security Center 14 Web Console

Por padrão, o Kaspersky Security Center usa certificados autoassinados (ou seja, emitidos pelo próprio Kaspersky Security Center), mas você pode substituí-los por certificados personalizados para melhor atender aos requisitos da rede da sua organização e cumprir os padrões de segurança. Depois que o Servidor de Administração verifica se um certificado personalizado atende a todos os requisitos aplicáveis, este certificado assume o mesmo escopo funcional de um certificado autoassinado. A única diferença é que um certificado personalizado não é reemitido automaticamente após a expiração. Você substitui certificados por certificados personalizados por meio do utilitário `klsetsrvcert` ou da seção de propriedades do Servidor de Administração no Kaspersky Security Center 14 Web Console, dependendo do tipo de certificado. Ao usar o utilitário `klsetsrvcert`, é preciso especificar um tipo de certificado usando um dos seguintes valores:

- C (certificado comum para as portas 13000 e 13291).
- CR (certificado de reserva comum para as portas 13000 e 13291).

Certificados do Servidor de Administração

Um certificado do Servidor de Administração é necessário para os seguintes propósitos:

- Autenticação de Servidor de Administração ao conectar-se ao Kaspersky Security Center 14 Web Console
- Interação segura entre o Servidor de Administração e o Agente de Rede em dispositivos gerenciados
- Autenticação quando os Servidores de Administração principais estão conectados aos Servidores de Administração secundários

O certificado do Servidor de Administração é criado automaticamente durante a instalação do componente do Servidor de Administração e é armazenado na pasta `/var/opt/kaspersky/klagent_srv/1093/cert/`. Você especifica o certificado do Servidor de Administração ao [criar um arquivo de resposta](#) para instalar o Kaspersky Security Center 14 Web Console. Este certificado é chamado comum ("C").

O certificado do Servidor de Administração é válido por 397 dias. O Kaspersky Security Center gera automaticamente um certificado de reserva comum (CR) 90 dias antes da expiração do certificado comum. O certificado de reserva comum é subsequentemente usado para a substituição perfeita do certificado do Servidor de Administração. Quando o certificado comum está prestes a expirar, o certificado de reserva comum é usado para manter a conexão com as instâncias do Agente de Rede instaladas nos dispositivos gerenciados. Com esta finalidade, o certificado de reserva comum torna-se automaticamente o novo certificado comum 24 horas antes de o antigo certificado comum expirar.

Se você especificar um prazo de validade superior a 397 dias para o certificado do Servidor de Administração, o navegador da Web retornará um erro.

Se necessário, você pode atribuir um certificado personalizado ao Servidor de Administração. Por exemplo, isso pode ser necessário melhorar a integração com o PKI existente da sua empresa ou para a configuração personalizada dos campos do certificado. Ao substituir o certificado, todos os Agentes de Rede que estiveram conectados anteriormente ao Servidor de Administração por meio do SSL perderão a conexão e retornarão o "Erro de autenticação do Servidor de Administração". Para eliminar o erro, será necessário restaurar a conexão após a [substituição do certificado](#).

Caso o certificado do Servidor de Administração tenha se perdido, é preciso reinstalar o componente Servidor de Administração e [restaurar os dados](#) para poder recuperá-lo.

Você também pode fazer backup do certificado do Servidor de Administração separadamente de outras configurações do Servidor de Administração para mover o Servidor de Administração de um dispositivo para outro, sem perda de dados.

Certificado do servidor da Web

Um tipo especial de certificado é usado pelo Servidor Web, um componente do Servidor de Administração do Kaspersky Security Center. Este certificado é necessário para publicar pacotes de instalação do Agente de Rede, que você baixa posteriormente para dispositivos gerenciados. Para isso, o Servidor Web pode usar vários certificados.

O Servidor Web usa um dos seguintes certificados, por ordem de prioridade:

1. Certificado de Servidor Web personalizado que você especificou manualmente por meio do Kaspersky Security Center 14 Web Console
2. Certificado do Servidor de Administração Comum ("C")

Certificado do Kaspersky Security Center 14 Web Console

O Servidor do Kaspersky Security Center 14 Web Console (aqui referido como Web Console) tem seu próprio certificado. Quando você abre um site, um navegador verifica se sua conexão é confiável. O certificado do Web Console permite autenticar o Web Console e é usado para criptografar o tráfego entre um navegador e o Web Console.

Quando o Web Console é aberto, o navegador pode informar que a conexão com o Web Console não é privada e o certificado do Web Console é inválido. Essa advertência aparece porque o certificado do Web Console é autoassinado e gerado automaticamente pelo Kaspersky Security Center. Para remover essa advertência, é possível fazer o seguinte:

- [Substitua o certificado do Web Console](#) por um personalizado (opção recomendada). Crie um certificado confiável na infraestrutura e que atenda aos [requisitos para certificados personalizados](#).
- Adicione o certificado do Web Console na lista de certificados de navegador confiáveis. Recomendamos usar essa opção somente se não puder criar um certificado personalizado.

Requisitos para certificados personalizados usados no Kaspersky Security Center

A tabela abaixo mostra os requisitos para [certificados personalizados especificados para diferentes componentes do Kaspersky Security Center](#).

Requisitos para certificados do Kaspersky Security Center

Tipo de certificado	Requisitos	Comentário
Certificado comum, certificado de reserva comum ("C", "CR")	<p>Comprimento mínimo da chave: 2048.</p> <p>Restrições básicas:</p> <ul style="list-style-type: none">• CA: true• Restrição de comprimento do caminho: nenhuma• Uso da chave:• Assinatura digital• Assinatura de certificado• Criptografia de chave• Assinatura CRL <p>Utilização estendida de chave (opcional): autenticação de servidor, autenticação de cliente.</p>	<p>O parâmetro Utilização estendida de chave é opcional.</p> <p>O valor da restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhuma", mas não inferior a "1".</p>
Certificado do servidor da Web	<p>Utilização estendida de chave: autenticação do servidor.</p> <p>O contêiner PKCS # 12 / PEM do qual o certificado é especificado inclui toda a cadeia de chaves públicas.</p> <p>O nome alternativo do assunto (SAN) do certificado está presente; ou seja, o valor do campo <code>subjectAltName</code> é válido.</p> <p>O certificado atende aos requisitos em vigor dos navegadores da web impostos aos certificados do servidor, bem como aos requisitos básicos atuais do Fórum CA / Navegador.</p>	Não aplicável.
Certificado do Kaspersky Security Center 14 Web Console	<p>O contêiner PEM do qual o certificado é especificado inclui toda a cadeia de chaves públicas.</p> <p>O nome alternativo do assunto (SAN) do certificado está presente; ou seja, o valor do campo <code>subjectAltName</code> é válido.</p> <p>O certificado atende aos requisitos em vigor de navegadores da web para certificados de servidor, bem como os requisitos básicos atuais do Fórum CA / Navegador.</p>	Certificados criptografados não são compatíveis com o Kaspersky Security Center 14 Web Console.

Reemissão do certificado do Kaspersky Security Center 14 Web Console

A maioria dos navegadores impõe um limite no prazo de validade de um certificado. Para se enquadrar neste limite, o prazo de validade do certificado do Kaspersky Security Center 14 Web Console é limitado a 397 dias. Você pode [substituir um certificado existente](#) recebido de uma autoridade de certificação (CA) emitindo um novo certificado autoassinado manualmente. Como alternativa, você pode emitir novamente o certificado expirado do Kaspersky Security Center 14 Web Console.

Quando o Web Console é aberto, o navegador pode informar que a conexão com o Web Console não é privada e o certificado do Web Console é inválido. Essa advertência aparece porque o certificado do Web Console é autoassinado e gerado automaticamente pelo Kaspersky Security Center. Para remover ou evitar esse aviso, é possível fazer o seguinte:

- Especifique um certificado personalizado ao reemiti-lo (opção recomendada). Crie um certificado confiável na infraestrutura e que atenda aos [requisitos para certificados personalizados](#).
- Adicione o certificado do Web Console na lista de certificados de navegador confiáveis depois de reemiti-lo. Recomendamos usar essa opção somente se não puder criar um certificado personalizado.

Para reemitir o certificado expirado do Kaspersky Security Center 14 Web Console:

Reinstale o Kaspersky Security Center 14 Web Console, executando uma das seguintes ações:

- Se você deseja usar o mesmo arquivo de instalação do Kaspersky Security Center 14 Web Console, remova o Kaspersky Security Center 14 Web Console e depois [instale a mesma versão do Kaspersky Security Center 14 Web Console](#).
- Se você deseja usar um arquivo de instalação de uma versão com upgrade, [execute o comando de upgrade](#).

O certificado do Kaspersky Security Center 14 Web Console é reemitido por outro período de validade de 397 dias.

Substituir o certificado do Kaspersky Security Center 14 Web Console

Por padrão, quando você instala o Kaspersky Security Center 14 Web Console Server (também conhecido como Kaspersky Security Center 14 Web Console), um certificado do navegador é automaticamente gerado. Você pode substituir o certificado automaticamente gerado por um certificado personalizado.

Para substituir o certificado do Kaspersky Security Center 14 Web Console por um certificado personalizado:

1. [Crie um novo arquivo de resposta](#) necessário para a instalação do Kaspersky Security Center 14 Web Console.
2. Neste arquivo, especifique o caminho para o arquivo de certificado personalizado e o arquivo de chave, usando o parâmetro certPath e keyPath.
3. Reinstale o Kaspersky Security Center 14 Web Console, especificando um novo arquivo de resposta. Execute uma das seguintes ações:
 - Se você deseja usar o mesmo arquivo de instalação do Kaspersky Security Center 14 Web Console, remova o Kaspersky Security Center 14 Web Console e depois [instale a mesma versão do Kaspersky Security Center 14 Web Console](#).

- Se você deseja usar um arquivo de instalação de uma versão com upgrade, [execute o comando de upgrade](#).

O Kaspersky Security Center 14 Web Console funciona com o certificado especificado.

Converter um certificado PFX para o formato PEM

Para usar um certificado PFX no Kaspersky Security Center 14 Web Console, você deve primeiro convertê-lo para o formato PEM usando qualquer utilitário multiplataforma baseado em OpenSSL conveniente.

Para converter um certificado PFX para o formato PEM no sistema operacional Linux:

1. Em um utilitário multiplataforma baseado em OpenSSL, execute os seguintes comandos:

```
openssl pkcs12 -in <nome do arquivo.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
```

```
openssl pkcs12 -in <nome do arquivo.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
```

2. Certifique-se de que o arquivo de certificado e a chave privada sejam gerados no mesmo diretório onde o arquivo .pfx está armazenado.
3. O Kaspersky Security Center 14 Web Console não oferece suporte a certificados protegidos por senha. Portanto, execute o seguinte comando em um utilitário multiplataforma baseado em OpenSSL para remover uma senha do arquivo .pem:

```
openssl rsa -in key.pem -out key-without-passphrase.pem
```

Não use o mesmo nome para os arquivos .pem de entrada e saída.

Como resultado, o novo arquivo .pem não é criptografado. Você não precisa inserir uma senha para usá-lo.

Os arquivos .crt e .pem estão prontos para uso, então você pode especificá-los no [instalador do Kaspersky Security Center 14 Web Console](#).

Cenário: especificação do certificado personalizado do Servidor de Administração

É possível atribuir o certificado personalizado do Servidor de Administração, por exemplo, para melhor integração com a infraestrutura de chave pública (PKI) existente de sua empresa ou para configuração personalizada dos campos de certificado. É útil substituir o certificado imediatamente após a instalação do Servidor de Administração e antes que o Assistente de Início Rápido for concluído.

Se você especificar um prazo de validade superior a 397 dias para o certificado do Servidor de Administração, o navegador da Web retornará um erro.

Pré-requisitos

O novo certificado deve ser criado no formato PKCS#12 (por exemplo, por meio da PKI da organização) e deve ser emitido por uma autoridade de certificação (CA) confiável. Além disso, o novo certificado deve incluir toda a cadeia de confiança e uma chave privada, que deve ser armazenada no arquivo com a extensão pfx ou p12. Para o novo certificado, os requisitos listados abaixo devem ser atendidos.

Tipo de certificado: certificado comum, certificado de reserva comum ("C", "CR")

Requisitos:

- Comprimento mínimo da chave: 2048
- Restrições básicas:
 - CA: true
 - Restrição de comprimento do caminho: nenhuma
O valor da Restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhuma", mas não inferior a "1".
- Uso da chave:
 - Assinatura digital
 - Assinatura de certificado
 - Criptografia de chave
 - Assinatura CRL
- Uso estendido de chave (EKU): autenticação de servidor e autenticação de cliente. O EKU é opcional, mas caso o seu certificado o contenha, os dados de autenticação do servidor e do cliente devem ser especificados no EKU.

Os certificados emitidos por uma CA pública não têm a permissão de assinatura de certificado. Para usar esses certificados, certifique-se de ter instalado o agente de rede versão 13 ou superior em pontos de distribuição ou gateways de conexão na rede. Caso contrário, não será possível usar os certificados sem a permissão de assinatura.

Fases

A especificação do certificado do Servidor de Administração prossegue em etapas:

1 Substituição do certificado do Servidor de Administração

Use a linha de comando do [utilitário klsetsrvcert](#) para este fim.

2 Especificação de um novo certificado e restauração da conexão de Agentes de Rede com o Servidor de Administração

Caso o certificado tenha sido substituído, todos os Agentes de Rede anteriormente conectados ao Servidor de Administração via SSL perderão a conexão e retornarão o "Erro de autenticação do Servidor de Administração." Para especificar o novo certificado e restaurar a conexão, use a linha de comando com o [utilitário klmover](#).

Resultados

Ao concluir o cenário, o certificado do Servidor de Administração é substituído e o servidor é autenticado pelos Agentes de Rede nos dispositivos gerenciados.

Substituição do certificado do Servidor de Administração usando o utilitário klsetsrvcert

Para substituir o certificado do Servidor de Administração:

Na linha de comando, execute o seguinte utilitário:

```
klsetsrvcert [-t <type> {-i <inputfile> [-p <password>] [-o <chkopt>] | -g <dnsname>}]  
[-f <time>][-r <calistfile>][-l <logfile>]
```

Não é preciso baixar o utilitário klsetsrvcert. Ele está incluído no kit de distribuição do Kaspersky Security Center. Não é compatível com versões anteriores do Kaspersky Security Center.

A descrição dos parâmetros do utilitário klsetsrvcert é apresentada na tabela abaixo.

Valores dos parâmetros do utilitário klsetsrvcert

Parâmetro	Valor
-t <type>	Tipo de certificado a ser substituído. Valores possíveis do parâmetro <type> : <ul style="list-style-type: none">• C – substitui o certificado para as portas 13000 e 13291.• CR – substitui o certificado reserva comum para as portas 13000 e 13291.
-f <time>	Cronograma de alteração do certificado, usando o formato “DD-MM-AAA hh:mm” (para portas 13000 e 13291). Use o parâmetro se quiser substituir o certificado reserva comum ou o certificado comum antes que ele expire. Especifique a hora em que os dispositivos gerenciados devem ser sincronizados com o Servidor de Administração em um novo certificado.
-i <inputfile>	Contêiner com o certificado e chave privada no formato PKCS#12 (arquivo com a extensão .p12 ou .pfx).
-p <password>	Senha usada para a proteção o contêiner p12. O certificado e uma chave privada são armazenados no contêiner, portanto, a senha é necessária para descriptografar o arquivo com o contêiner.
-o <chkopt>	Parâmetros de validação de certificado (separados por ponto e vírgula). Para usar um certificado personalizado sem a permissão de assinatura, especifique -o NoCA no utilitário klsetsrvcert. Isso é útil para certificados emitidos por uma CA pública.
-g <dnsname>	Um novo certificado será criado para o nome DNS especificado.
-r <calistfile>	Lista de autoridades de certificado raiz confiáveis, formato PEM.
-l <logfile>	Arquivo de saída dos resultados. Por padrão, a saída é redirecionada no fluxo de saída padrão.

Por exemplo, para especificar o [certificado personalizado do Servidor de Administração](#), use o seguinte comando:

```
klsetsrvcert -t C -i <inputfile> -p <password> -o NoCA
```

Após a substituição do certificado, todos os Agentes de Rede conectados com Servidor de Administração por meio de SSL perdem a conexão. Para restaurá-la, use a linha de comando do [utilitário klmover](#).

Conexão dos Agentes de Rede ao Servidor de Administração usando o utilitário klmover

Depois de substituir o certificado do Servidor de Administração usando a linha de comando do [utilitário klsetsrvcert](#), é preciso estabelecer a conexão SSL entre os Agentes de Rede e o Servidor de Administração porque a conexão foi interrompida.

Para especificar o novo certificado do Servidor de Administração e restaurar a conexão:

Na linha de comando, execute o seguinte utilitário:

```
klmover [-address <endereço do servidor>] [-pn <número da porta>] [-ps <número da porta SSL>] [-noss1] [-cert <caminho para arquivo de certificado>]
```

O utilitário é copiado automaticamente para a pasta de instalação do agente de rede, quando ele é instalado em um dispositivo cliente.

A descrição dos parâmetros do utilitário klmover é apresentada na tabela abaixo.

Valores dos parâmetros do utilitário klmover

Parâmetro	Valor
-address <server address>	Endereço do Servidor de Administração para conexão. É possível especificar um endereço IP ou o nome DNS.
-pn <número da porta>	Número da porta pela qual a conexão não criptografada será estabelecida com Servidor de Administração. O número da porta padrão é 14000.
-ps <número da porta SSL>	Número da porta SSL pela qual a conexão criptografada será estabelecida com o Servidor de Administração usando o protocolo SSL. O número da porta padrão é 13000.
-noss1	Usa a conexão não criptografada com Servidor de Administração. Caso a chave não esteja sendo usada, o agente de rede é conectado ao Servidor de Administração usando o protocolo SSL codificado.
-cert <path to certificate file>	Usa o arquivo de certificado especificado para autenticação de acesso com o Servidor de Administração.

Definir uma pasta compartilhada

Após a instalação do Servidor de Administração, é possível especificar o local da pasta compartilhada nas propriedades do Servidor de Administração. Por padrão, a pasta compartilhada é criada no dispositivo com o Servidor de Administração. No entanto, em alguns casos (como alta carga ou a necessidade para o acesso a partir de uma rede isolada), é útil localizar a pasta compartilhada em um recurso de arquivo dedicado.

A pasta compartilhada é usada ocasionalmente na implementação de Agente de Rede.

A diferenciação entre maiúsculas e minúsculas para a pasta compartilhada deve estar desativada.

Sobre atualizar o Kaspersky Security Center Linux

Você pode instalar a versão 14 do Servidor de Administração em um dispositivo que tenha uma versão anterior do Servidor de Administração instalada (a partir da versão 13). Ao atualizar para a versão 14, todos os dados e configurações da versão anterior do Servidor de Administração são salvos.

Durante a atualização, o uso simultâneo do DBMS pelo Servidor de Administração e outro aplicativo é estritamente proibido.

É possível atualizar uma versão do Servidor de Administração usando um dos seguintes métodos:

- Ao usar o [arquivo de instalação do Kaspersky Security Center](#)
- Ao criar o [backup de dados do Servidor de Administração](#), instalando uma nova versão do Servidor de Administração e restaurando os dados do Servidor de Administração do backup

Se sua rede incluir vários Servidores de Administração, você deverá atualizar cada Servidor manualmente. O Kaspersky Security Center Linux não oferece suporte à atualização centralizada.

Ao atualizar o Kaspersky Security Center Linux de uma versão anterior, todos os plugins instalados dos aplicativos compatíveis são mantidos. O plugin do Servidor de Administração e o agente do Network Agent são atualizados automaticamente.

Atualizar o Kaspersky Security Center Linux usando o arquivo de instalação

Para atualizar o Servidor de Administração de uma versão anterior (a partir da versão 13) para a versão 14, você pode instalar uma nova versão sobre uma anterior usando o arquivo de instalação do Kaspersky Security Center.

Para atualizar uma versão anterior do Servidor de Administração para a versão 14 usando o arquivo de instalação:

1. Baixe o arquivo de instalação do Kaspersky Security Center com um pacote completo para a versão 14 no site da Kaspersky:
 - Para dispositivos que executam um sistema operacional baseado em RPM, `ksc64-<número da versão>-11247.x86_64.rpm`
 - Para dispositivos que executam um sistema operacional baseado em Debian, `ksc64-<número da versão>-11247_amd64.deb`
2. Atualize o pacote de instalação usando um gerenciador de pacotes que você usa em seu Servidor de Administração. Por exemplo, você pode usar os seguintes comandos no terminal de linha de comando em uma conta com privilégios de acesso a raiz:
 - Para os dispositivos que executam um sistema operacional baseado em RPM:
`$ sudo rpm -Uvh --nodeps --force ksc64-<número da versão>-11247.x86_64.rpm`
 - Para os dispositivos com um sistema operacional baseado em Debian:
`$ sudo dpkg -i ksc64-<número da versão>-11247_amd64.deb`

Após a execução bem-sucedida do comando, o script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` será criado. A mensagem sobre isso será exibida no terminal.

3. Execute o script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` para configurar o Servidor de Administração atualizado.
4. Leia o Contrato de Licença e a Política de Privacidade, que aparecem no terminal de linha de comando. Se você concordar com todos os termos do Contrato de Licença e da Política de Privacidade:

- a. Digite "Y" para confirmar que você leu, entendeu e aceita totalmente os termos e as condições do EULA.
- b. Digite "Y" novamente para confirmar que você leu, entendeu e aceita totalmente a Política de Privacidade que descreve o tratamento de dados.

A Instalação do aplicativo no seu dispositivo continuará após você inserir "Y" duas vezes.

5. Digite "1" para selecionar o modo de instalação padrão do Servidor de Administração.

A imagem abaixo mostra as duas últimas etapas.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

ACEITAR OS TERMOS DO EULA E DA POLÍTICA DE PRIVACIDADE E SELECIONAR O MODO DE INSTALAÇÃO PADRÃO DO SERVIDOR DE ADMINISTRAÇÃO NO TERMINAL DE LINHA DE COMANDO

Em seguida, o script configura e conclui a atualização do Servidor de Administração. Durante a atualização, não é possível alterar as configurações do Servidor de Administração ajustadas antes da atualização.

6. Para dispositivos nos quais uma versão anterior do Agente de Rede estiver instalada, crie e execute a tarefa para instalação remota da nova versão do Agente de Rede.

Recomendamos atualizar o Agente de Rede para Linux para a mesma versão do Kaspersky Security Center Linux.

Após a conclusão da tarefa de instalação remota, a versão do Agente de Rede será atualizada.

Atualizar o Kaspersky Security Center Linux por meio de backup

Para atualizar o Servidor de Administração de uma versão anterior (a partir da versão 13) para a versão 14, você pode criar um backup dos dados do Servidor de Administração e restaurar esses dados após instalar o Kaspersky Security Center de uma nova versão. Se problemas ocorrerem durante a instalação, você poderá restaurar a versão anterior do Servidor de Administração por meio do uso do backup dos dados do Servidor de Administração criados antes da atualização.

Para atualizar uma versão anterior do Servidor de Administração para a versão 14 por meio do backup:

1. Antes da atualização, [faça backup dos dados do Servidor de Administração](#) com uma versão mais antiga do aplicativo.

2. Desinstale a versão mais antiga do Kaspersky Security Center.
3. [Instale o Kaspersky Security Center versão 14](#) no antigo Servidor de Administração.
4. [Restaure os dados do Servidor de Administração](#) do backup criado antes da atualização.
5. Para dispositivos nos quais uma versão anterior do Agente de Rede estiver instalada, crie e execute a tarefa para instalação remota da nova versão do Agente de Rede.

Recomendamos atualizar o Agente de Rede para Linux para a mesma versão do Kaspersky Security Center Linux.

Após a conclusão da tarefa de instalação remota, a versão do Agente de Rede será atualizada.

Login no Kaspersky Security Center 14 Web Console e logout

Você pode fazer login no Kaspersky Security Center 14 Web Console após [instalar o Servidor de Administração e o Web Console Server](#). Você deve saber o endereço da Web do Servidor de Administração e o número de porta especificado durante a instalação (por padrão, a porta é 8080). No navegador, o JavaScript deve ser ativado.

Para efetuar o login no Kaspersky Security Center 14 Web Console:

1. No navegador, vá para <endereço da Web do Servidor de Administração>:<Número da porta>.

A página de login é exibida.

2. Se tiver adicionado vários servidores confiáveis, selecione, na lista Servidores de Administração, o Servidor de Administração ao qual deseja se conectar.

Se você tiver adicionado apenas um Servidor de Administração, apenas os campos Login e Senha serão exibidos.

3. Execute uma das seguintes ações:

- Para efetuar login no Servidor de Administração físico, digite o nome de usuário e a senha do Administrador local.
- Se um ou mais Servidores de Administração virtuais forem criados no Servidor e você desejar efetuar login em um Servidor virtual:
 - a. Clique em **Configurações avançadas**.
 - b. Digite o nome do Servidor de Administração virtual que você especificou enquanto [criava o servidor virtual](#).
 - c. Digite o nome de usuário e a senha do administrador que tem direitos no Servidor de Administração virtual.

Após o login, o painel será exibido contendo o idioma e o tema que você usou pela última vez. Você pode navegar pelo Kaspersky Security Center 14 Web Console e usá-lo para trabalhar com o Kaspersky Security Center Linux.

Para efetuar o logout do Kaspersky Security Center 14 Web Console:

1. Clique no seu nome de usuário no canto superior direito da tela.

2. No menu suspenso, selecione **Sair**.

O Kaspersky Security Center 14 Web Console é fechado, e a página de login é exibida.

Assistente de Início Rápido

O Kaspersky Security Center Linux lhe permite ajustar uma seleção mínima de configurações necessárias para criar um sistema de gerenciamento centralizado para proteger a rede contra ameaças à segurança. Esta configuração é executada através do Assistente de Início Rápido. Quando o Assistente estiver em execução, você pode fazer as seguintes modificações ao aplicativo:

- Adicione arquivos de chaves ou insira códigos de ativação que podem ser distribuídas automaticamente para os dispositivos dentro de grupos de administração.
- Defina entrega de notificações por e-mail sobre os eventos que ocorrem durante a operação do Servidor de Administração e de aplicativos gerenciados (a entrega com êxito da notificação requer que o serviço Messenger continue a estar em execução no Servidor de Administração e nos dispositivos de todos os destinatários).
- Crie uma política de proteção para estações de trabalho e servidores, assim como tarefas de verificação de vírus, tarefas de download de atualização e tarefas de backup dos dados, para o nível superior da hierarquia de dispositivos gerenciados.

O Assistente de Início Rápido cria políticas somente para aplicativos para os quais a pasta **DISPOSITIVOS GERENCIADOS** não contém nenhuma política. O Assistente de Início Rápido não cria tarefas se algumas já tiverem sido criadas com os mesmos nomes para o nível superior da hierarquia dos dispositivos gerenciados.

O aplicativo solicita automaticamente que você execute o Assistente de Início Rápido após a instalação do Servidor de Administração, na primeira conexão a ele. Você também pode iniciar o Assistente de Início Rápido manualmente a qualquer momento.

Para iniciar o Assistente de Início Rápido manualmente:

1. Na janela de aplicativo principal, clique no ícone **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 Assistente de Início Rápido**.

O Assistente solicita que você execute a configuração inicial do Servidor de Administração. Siga as instruções do Assistente. Prossiga pelo Assistente usando o botão **Avançar**.

Etapa 1. Especificando as configurações de conexão da Internet

Especifique as configurações de acesso à Internet para o Kaspersky Security Center Linux.

Selecione a caixa de seleção **Usar o servidor proxy** se você quiser usar um servidor proxy ao se conectar à Internet. Se essa caixa de seleção estiver marcada, os campos estão disponíveis para inserir configurações. Especifique as seguintes configurações para a conexão ao servidor proxy:

- **Endereço**

- Número da porta


- [Ignorar servidor proxy para endereços locais](#) 

Nenhum servidor proxy será usado para conectar-se aos dispositivos na rede local.

- [Autenticação do servidor proxy](#) 

Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

Este campo de entrada está disponível se a caixa de seleção **Usar o servidor proxy** estiver marcada.

- [Nome do usuário](#)  (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada)

Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

- [Senha](#)  (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada)

A senha definida pelo usuário de cuja conta a conexão com o servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

Para ver a senha inserida, mantenha pressionado o botão **Exibir** pelo tempo que você desejar.

Passo 2. Selecionando o método de ativação do aplicativo

Selecione uma das seguintes opções de ativação do Kaspersky Security Center Linux:

- [Inserindo o seu código de ativação](#) 

Código de ativação é uma sequência única de 20 caracteres alfanuméricos. Você insere um código de ativação para adicionar uma chave que ativa o Kaspersky Security Center Linux. Você recebe o código de ativação através do endereço de e-mail especificado após a compra do Kaspersky Security Center.

Para ativar o aplicativo com um código de ativação, você precisa de acesso à Internet para estabelecer a conexão com os servidores de ativação da Kaspersky.

Se você selecionou essa opção de ativação, pode ativar a opção **Automaticamente implementar chave de licença nos dispositivos gerenciados**.

Se esta opção estiver ativada, a chave de licença será implementada automaticamente para os dispositivos gerenciados.

Se esta opção estiver desativada, você poderá implantar a chave de licença em dispositivos gerenciados posteriormente na seção **OPERAÇÕES** → **LICENCIAMENTO** → **LICENÇAS DA KASPERSKY** do menu principal.

- [Especificando um arquivo de chave](#) 

O *Arquivo de chave* é um arquivo com a extensão .key fornecido a você pela Kaspersky. O objetivo do arquivo de chave é adicionar uma chave que ativa o aplicativo.

Você recebe o arquivo de chave via endereço de e-mail especificado após a compra do Kaspersky Security Center.

Para ativar o aplicativo usando um arquivo de chave, não é necessário conectar-se aos servidores de ativação da Kaspersky.

Se você selecionou essa opção de ativação, pode ativar a opção **Automaticamente implementar chave de licença nos dispositivos gerenciados**.

Se esta opção estiver ativada, a chave de licença será implementada automaticamente para os dispositivos gerenciados.

Se esta opção estiver desativada, você poderá implantar a chave de licença em dispositivos gerenciados posteriormente na seção **OPERAÇÕES** → **LICENCIAMENTO** → **LICENÇAS DA KASPERSKY** do menu principal.

- Ao adiar a ativação do aplicativo

Se você decidiu adiar a ativação do aplicativo, poderá adicionar uma chave de licença depois a qualquer momento selecionando **OPERAÇÕES** → **LICENCIAMENTO**.

Ao trabalhar com o Kaspersky Security Center implementado a partir de uma AML paga ou uma SKU com base no uso e faturamento mensal, você não pode especificar um arquivo de chave ou inserir um código.

Etapa 3. Criar uma configuração de proteção de rede básica

Você poderá verificar a lista de políticas e tarefas que foram criadas.

Espere pela conclusão da criação de políticas e tarefas antes de prosseguir à etapa seguinte do Assistente.

Etapa 4. Configurar as notificações por e-mail

Configure a entrega de notificações sobre os eventos registrados durante a operação dos aplicativos Kaspersky em dispositivos cliente. Essas configurações serão usadas como as configurações padrão para as políticas de aplicativo.

Para configurar a entrega de notificações sobre os eventos que ocorrem nos aplicativos Kaspersky, use as seguintes configurações:

- [Destinatários \(endereços de e-mail\)](#) ²

Os endereços de e-mail de usuários aos quais o aplicativo enviará notificações. Você pode inserir um ou vários endereços; se inserir mais de um endereço, separe-os com um ponto-e-vírgula.

- [Endereço do servidor SMTP](#) ²

O endereço ou os endereços dos servidores de e-mail da sua organização.

Se você inserir mais de um endereço, separe-os com um ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome de DNS do servidor SMTP

- [Porta do servidor SMTP](#)

Número da porta de comunicação do servidor SMTP. O número da porta padrão é 25.

- [Usar a autenticação ESMTP](#)

Ativa o suporte da autenticação ESMTP. Após selecionar a caixa de seleção, nos campos **Nome do usuário** e **Senha**, você poderá especificar as configurações de autenticação ESMTP. Por padrão, esta caixa de seleção está desmarcada, e as configurações da autenticação ESMTP não estão disponíveis.

Você pode testar as novas configurações de notificação por e-mail clicando no botão **Enviar mensagem de teste**.

Etapa 5. Fechar o Assistente de Início Rápido

Para fechar o Assistente, pressione o botão **Concluir**.

Depois de concluir o Assistente de Início Rápido, será possível executar o [Assistente de Implementação da Proteção](#) para instalar automaticamente os aplicativos de antivírus ou Agente de Rede nos dispositivos de sua rede.

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 da 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**.

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.

Iniciar o Assistente de Implementação da Proteção

Você pode iniciar o Assistente de Implementação da Proteção a qualquer momento.

Para iniciar o Assistente de Implementação da Proteção manualmente,

Na janela principal do aplicativo, clique em **DESCOBERTA E IMPLEMENTAÇÃO** → **IMPLEMENTAÇÃO E ATRIBUIÇÃO** → **ASSISTENTE DE IMPLEMENTAÇÃO DA 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 um método de distribuição de arquivo de chave ou código de ativação

Selecione um método para a distribuição de arquivo de chave ou do código de ativação:

- [Não adicionar chave de licença ao pacote de instalação](#) 

A chave será automaticamente distribuída a todos os dispositivos com os quais ela for compatível:

- Se a distribuição automática foi ativada nas propriedades da chave.
- Se a tarefa **Adicionar chave** foi criada.

- [Adicionar chave de licença ao pacote de instalação](#) 

A chave é distribuída aos dispositivos em conjunto com o pacote de instalação.

Não recomendamos que distribua a chave usando este método, porque os direitos de acesso de Leitura são ativados para o repositório de pacotes de instalação.

Se o pacote de instalação já incluir um arquivo de chave ou código de ativação, essa janela será exibida, mas conterá apenas os detalhes da chave de licença.

Etapa 3. 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 4. 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 5. 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.

Se esta opção estiver desativada, os pacotes de instalação serão entregues usando as ferramentas do sistema operacional Linux.

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 **Usando 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 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 Linux Center 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 \(Agente de Rede não é usado\)](#) [?]

Se essa caixa de seleção estiver selecionada, você poderá especificar uma conta sob a qual o instalador do aplicativo será executado. Você poderá especificar a conta do usuário se o Agente de Rede não estiver instalado nos dispositivos para os quais a tarefa foi atribuída.

Você pode especificar múltiplas contas de usuário se, por exemplo, nenhuma delas tiver os direitos necessários em todos os dispositivos para os quais a tarefa foi atribuída. Nesse caso, todas as contas que foram adicionadas são usadas para executar a tarefa, por ordem consecutiva, de cima para baixo.

Se nenhuma conta for adicionada, a tarefa será executada na conta em que o serviço do Servidor de Administração está sendo executado.

Etapa 9. Iniciando a 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 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.

Configurando o Servidor de Administração

Esta seção descreve o processo de configuração e as propriedades do Servidor de Administração do Kaspersky Security Center Linux.

Configuração da conexão do Kaspersky Security Center 14 Web Console ao Servidor de Administração

Para definir as portas de conexão do Servidor de Administração:

1. Na parte superior da tela, 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 **Portas de conexão**.

O aplicativo exibe as configurações de conexão principais do servidor selecionado.

Configurando uma lista de permissão de endereços IP para fazer login no Kaspersky Security Center

Por padrão, os usuários podem fazer login no Kaspersky Security Center em qualquer dispositivo onde possam abrir o Kaspersky Security Center 14 Web Console (também chamado de Web Console). No entanto, é possível configurar o Servidor de Administração para que os usuários possam se conectar a ele apenas a partir de dispositivos com endereços IP permitidos. Nesse caso, mesmo que um invasor roube uma conta do Kaspersky Security Center, ele não poderá fazer login no Kaspersky Security Center porque o endereço IP do dispositivo do invasor não está na lista de permissão.

O endereço IP é verificado quando um usuário faz login no Kaspersky Security Center ou executa um [aplicativo @](#) que interage com o Servidor de Administração via [Kaspersky Security Center OpenAPI](#). Neste momento, o dispositivo de um usuário tenta estabelecer uma conexão com o Servidor de Administração. Caso o endereço IP do dispositivo não esteja na lista de permissão, ocorrerá um erro de autenticação e o [evento KLAUD_EV_SERVERCONNECT](#) notifica que uma conexão com o Servidor de Administração não foi estabelecida.

Requisitos para uma lista de permissão de endereços IP

Os endereços IP são verificados apenas quando os seguintes aplicativos tentam se conectar ao Servidor de Administração:

- Web Console Server

Caso entre no Kaspersky Security Center por meio do Web Console, será possível configurar um firewall no dispositivo em que o Servidor do Console da Web está instalado usando os meios padrão do sistema operacional. Então, caso alguém tente fazer login no Kaspersky Security Center em um dispositivo e o Web Console Server for [instalado em outro dispositivo](#), um firewall ajudará a evitar a interferência de invasores.

- Aplicativos com interação com o Servidor de Administração por meio de objetos de automação klakaut

- Aplicativos que interagem com o Servidor de Administração via OpenAPI, como Kaspersky Anti Targeted Attack Platform ou Kaspersky Security for Virtualization

Portanto, especifique os endereços dos dispositivos nos quais os aplicativos listados acima estão instalados.

É possível definir os endereços IPv4 e IPv6. Não é possível especificar os intervalos de endereços IP.

Como estabelecer uma lista de permissão de endereços IP

Caso não tenha definido uma lista de permissão anteriormente, siga as instruções abaixo.

Para estabelecer uma lista de permissão de endereços IP para fazer login no Kaspersky Security Center:

1. No dispositivo do Servidor de Administração, execute o prompt de comando do Windows em uma conta com direitos de administrador.
2. Altere o diretório atual para a pasta de instalação do Kaspersky Security Center (geralmente, /opt/kaspersky/ksc64/sbin).

3. Digite o seguinte comando, usando direitos de administrador:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<endereços IP>" -t s
```

Especifique os endereços IP que atendem aos requisitos listados acima. Muitos endereços IP devem ser separados por um ponto e vírgula.

Exemplo de como permitir que apenas um dispositivo se conecte ao Servidor de Administração:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s
```

Exemplo de como permitir que vários dispositivos se conectem ao Servidor de Administração:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
```

4. Reinicie o serviço do Servidor de Administração.

É possível descobrir se a lista de permissão de endereços IP no Log de Eventos do Syslog do Servidor de Administração foi configurada com êxito.

Como alterar uma lista de permissão de endereços IP

É possível alterar uma lista de permissão exatamente como foi feito na primeira vez. Para isso, execute o mesmo comando e especifique uma nova lista de permissão:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<endereços IP>" -t s
```

Caso queira excluir alguns endereços IP da lista de permissão, basta reescrevê-los. Por exemplo, a lista de permissão inclui os seguintes endereços IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. O usuário deseja excluir o endereço IP 198.51.100.0. Para fazer isso Digite o seguinte comando no prompt de comando:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Não se esqueça de reiniciar o serviço do Servidor de Administração.

Como redefinir uma lista de permissão de endereços IP configurada

Para redefinir uma lista de permissão de endereços IP já configurada:

1. Digite o seguinte comando no prompt de comando do Windows, usando direitos de administrador:
`klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. Reinicie o serviço do Servidor de Administração.

Depois disso, os endereços IP não serão mais verificados.

Visualização do registro das conexões com o Servidor de Administração

O histórico das conexões e tentativas de conexão ao Servidor de Administração durante a operação pode ser salvo em um arquivo de registro. As informações no arquivo permitem que você rastreie não só as conexões dentro sua infraestrutura de rede, mas também as tentativas não autorizadas de acessar o servidor.

Para registrar eventos da conexão ao Servidor de Administração:

1. Na janela principal do aplicativo, clique no ícone **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 **Portas de conexão**.

3. Ative a opção **Criar log de eventos de conexão do Servidor de Administração**.

Todos os eventos adicionais das conexões de entrada com o Servidor de Administração, resultados de autenticação e erros de SSL serão salvos no arquivo %ProgramData%\KasperskyLab\adminikit\logs\sc.syslog.

Configuração do número máximo de eventos no repositório de eventos

Na seção **Repositório de eventos** da janela Propriedades do Servidor de Administração, você pode editar as configurações de armazenamento do evento no banco de dados do Servidor de Administração ao limitar o número de registros de evento ou o tempo de armazenamento do registro. Quando você especifica o número máximo de eventos, o aplicativo calcula um volume aproximado do espaço de armazenamento necessário para o número especificado. Você pode usar esse cálculo aproximado para avaliar se você tem espaço livre suficiente no disco para evitar sobrecarga do banco de dados. A capacidade padrão do banco de dados do Servidor de Administração é de 400.000 eventos. A capacidade máxima recomendada do banco de dados é de 45 milhões de eventos.

Se o número de eventos no banco de dados atingir o valor máximo especificado pelo administrador, o aplicativo exclui os eventos mais antigos o regravando com os novos eventos. Quando o Servidor de Administração exclui eventos antigos, não pode salvar novos eventos no banco de dados. Durante esse período de tempo, as informações sobre eventos rejeitados são gravadas no Log de Eventos Kaspersky. Os novos eventos são colocados em fila e salvos no banco de dados depois que a operação de exclusão é concluída.

Para limitar o número de eventos que podem ser armazenados no repositório de eventos no Servidor de Administração:

1. Na parte superior da tela, 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 **Repositório de eventos**. Especifique o número máximo de eventos armazenados no banco de dados.
3. Clique no botão **Salvar**.

Cópia backup e restauração dos dados do Servidor de Administração

O backup de dados permite mover um Servidor de Administração de um dispositivo para outro, sem perda de dados. Usando o backup, você pode restaurar dados ao mover o banco de dados de um Servidor de Administração para outro dispositivo ou ao atualizar para uma versão mais recente do Kaspersky Security Center.

Observe que não é feito backup dos plugins de gerenciamento instalados. Depois de restaurar os dados do Servidor de Administração a partir de uma cópia backup, você precisará fazer download e reinstalar plug-ins para aplicativos gerenciados.

Você pode criar uma cópia backup dos dados do Servidor de Administração em uma das seguintes formas:

- Criando e executando uma [tarefa de backup de dados](#) através do Kaspersky Security Center 14 Web Console.
- Executando o [utilitário klbackup](#) no dispositivo que tenha o Servidor de Administração instalado. Este utilitário está incluído no kit de distribuição do Kaspersky Security Center. Após a instalação do Servidor de Administração, o utilitário estará localizado na raiz da pasta de destino especificada na instalação do aplicativo (geralmente /opt/kaspersky/ksc64/sbin/klbackup).

Os seguintes dados são salvos em uma cópia backup do Servidor de Administração:

- O banco de dados do Servidor de Administração (políticas, tarefas, configurações de aplicativo, eventos salvos no Servidor de Administração).
- Detalhes da configuração da estrutura dos grupos de administração e dispositivos cliente.
- Repositório dos pacotes de distribuição de aplicativos para a instalação remota.
- Certificado do Servidor de Administração.

A recuperação dos dados do Servidor de Administração só é possível usando o utilitário klbackup.

Criando uma tarefa de backup de dados do Servidor de Administração

As tarefas de backup são tarefas do Servidor de Administração, criadas através do [Assistente de Início Rápido](#). Se uma tarefa de backup criada pelo Assistente de Início Rápido tiver sido excluída, você pode criar uma manualmente.

A tarefa *Backup de dados do Servidor de Administração* só pode ser criada numa única cópia. Se a tarefa de backup de dados do Servidor de Administração já foi criada para o Servidor de Administração, ela não é exibida na janela de seleção de tipo de tarefa.

Para criar uma tarefa de backup de dados do Servidor de Administração:

1. Acesse **DISPOSITIVOS** → **TAREFAS**.
2. Clique em **Adicionar**.
 - Assistente para Adicionar Tarefas é iniciado.
3. Na primeira página do Assistente, na lista **Aplicativo**, selecione **Kaspersky Security Center 14**, e na lista **Tipo de tarefa**, selecione **Backup de dados do Servidor de Administração**.
4. Na página correspondente do Assistente, especifique as seguintes informações:
 - Pasta para armazenamento de cópias de backup
 - Senha para backup (opcional)
 - Número máximo de cópias de backup a salvar
5. 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.
6. Clique no botão **Concluir**.

A tarefa é criada e exibida na lista de tarefas.

Utilitário de backup de dados e recuperação (klbackup)

Você copiar os dados do Servidor de Administração para backup e recuperação futura, usando o utilitário klbackup, que está incluído no kit de distribuição do Kaspersky Security Center.

O utilitário klbackup pode ser executado em qualquer um dos seguintes modos:

- [Interativo](#)
- [Não interativo](#)

Backup de dados e recuperação no modo interativo

Para criar uma cópia backup dos dados do Servidor de Administração no modo interativo:

1. Execute o utilitário klbackup localizado na pasta de instalação do Kaspersky Security Center (geralmente, `/opt/kaspersky/ksc64/sbin/klbackup`).
 - Assistente de Backup e Restauração é iniciado.

2. Na primeira página do Assistente, selecione **Executar backup dos dados do Servidor de Administração**.

Se você selecionar a opção **Restaurar ou fazer backup somente do certificado do Servidor de Administração**, somente uma cópia backup do certificado do Servidor de Administração será salva.

Clique em **Avançar**.

3. Na janela seguinte do assistente, especifique uma senha e uma pasta de destino para o backup e clique no botão **Avançar** para iniciar o backup.

Para recuperar os dados do Servidor de Administração no modo interativo:

1. Execute o utilitário `klbackup` localizado na pasta de instalação do Kaspersky Security Center (geralmente, `/opt/kaspersky/ksc64/sbin/klbackup`). Inicie o utilitário na mesma conta em que você instalou o Servidor de Administração.

O Assistente de Backup e Restauração é iniciado.

2. Na primeira página do Assistente, selecione **Restaurar dados do Servidor de Administração**.

Se você selecionar a opção **Restaurar ou fazer backup somente do certificado do Servidor de Administração**, apenas o certificado do Servidor de Administração será recuperado.

Clique em **Avançar**.

3. Na janela **Restaurar configurações** do Assistente:

- Especifique a pasta que contém uma cópia backup dos dados do Servidor de Administração. Você deve certificar-se de que o nome do arquivo é `backup.zip`.
- Especifique a senha que foi inserida durante o backup dos dados.

Ao restaurar dados, você deve especificar a mesma senha que foi inserida durante o backup. Se o caminho para uma pasta compartilhada for alterado após o backup, verifique a operação de tarefas que usam os dados restaurados (tarefas de restauração e tarefas de instalação remota). Se necessário, edite as configurações dessas tarefas. Enquanto os dados estão sendo restaurados de um arquivo de backup, ninguém deve acessar a pasta compartilhada do Servidor de Administração. A conta em que o utilitário `klbackup` é iniciado deve ter acesso completo à pasta compartilhada.

4. Clique no botão **Avançar** para restaurar os dados.

Backup de dados e recuperação no modo não interativo

Para criar uma cópia de backup ou recuperar os dados do Servidor de Administração no modo não interativo,

Execute o utilitário `klbackup` com o conjunto de chaves a partir da linha de comando de um dispositivo que tenha o Servidor de Administração instalado.

A sintaxe da linha de comando do utilitário:

```
klbackup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts][[-restore] [-password PASSWORD] [-online]
```

Se nenhuma senha for especificada na linha de comando do utilitário `klbackup`, o utilitário solicita a inserção da senha interativamente.

Descrições das chaves:

- `-path BACKUP_PATH` — Salve as informações na pasta `BACKUP_PATH` ou use os dados da pasta `BACKUP_PATH` para a recuperação (parâmetro obrigatório).
- `-logfile LOGFILE` — Salve um relatório no backup de dados e recuperação do Servidor de Administração. Devem ser concedidas permissões à conta do servidor do banco de dados e ao utilitário `klbackup` para alterar os dados na pasta `BACKUP_PATH`.
- `-use_ts` — Quando estiver salvando os dados, copie as informações na pasta `BACKUP_PATH`, na subpasta com um nome contendo a data e hora de operação atuais do sistema no formato `klbackup YYYY-MM-DD # HH-MM-SS`. Se nenhuma chave for especificada, as informações são salvas na raiz da pasta `BACKUP_PATH`.
Ao tentar salvar informações em uma pasta que já armazena uma cópia backup, uma mensagem de erro será exibida. Nenhuma informação será atualizada.
A disponibilidade da chave `-use_ts` permite manter um arquivo de dados do Servidor de Administração. Por exemplo, se a chave `-path` indicar a pasta `C:\KLBackups`, a pasta `klbackup 2022/6/19 # 11-30-18` armazenará as informações sobre o status do Servidor de Administração em 19 de junho de 2022, às 11:30:18.
- `-restore` — Recupere os dados do Servidor de Administração. A recuperação de dados é realizada com base nas informações contidas na pasta `BACKUP_PATH`. Se não houver nenhuma chave, um backup dos dados é feito na pasta `BACKUP_PATH`.
- `-password PASSWORD` — Salve ou recupere o certificado do Servidor de Administração; para criptografar e descriptografar; use a senha especificada pelo parâmetro `PASSWORD`.

Uma senha esquecida não pode ser recuperada. Não há requisitos de senha. O comprimento da senha é ilimitado e também é possível um comprimento nulo (sem senha).

Ao restaurar dados, você deve especificar a mesma senha que foi inserida durante o backup. Se o caminho para uma pasta compartilhada for alterado após o backup, verifique a operação de tarefas que usam os dados restaurados (tarefas de restauração e tarefas de instalação remota). Se necessário, edite as configurações dessas tarefas. Enquanto os dados estão sendo restaurados de um arquivo de backup, ninguém deve acessar a pasta compartilhada do Servidor de Administração. A conta em que o utilitário `klbackup` é iniciado deve ter acesso completo à pasta compartilhada.

- `-online` — Backup dos dados do Servidor de Administração ao criar um instantâneo do volume para, diminuir o tempo offline do Servidor de Administração. Quando você usa o utilitário para recuperar os dados, esta opção é ignorada.

Mover o Servidor de Administração e um servidor de banco de dados para outro dispositivo

Se precisar usar o Servidor de Administração em um novo dispositivo, poderá movê-lo de uma das seguintes maneiras:

- Mova o Servidor de Administração e um servidor de banco de dados para um novo dispositivo.
- Mantenha o servidor de banco de dados no dispositivo anterior e mova apenas o Servidor de Administração para um novo dispositivo.

Para mover o Servidor de Administração e um servidor de banco de dados para um novo dispositivo:

1. No dispositivo anterior, crie um backup de dados do Servidor de Administração.

Para fazer isso, você pode executar a [tarefa de backup de dados](#) por meio do Kaspersky Security Center 14 Web Console ou executar o [utilitário klbackup](#).

2. Selecione um novo dispositivo no qual instalar o Servidor de Administração. Certifique-se de que o hardware e o software do dispositivo selecionado atendam aos [requisitos](#) para Servidor de Administração, Kaspersky Security Center 14 Web Console e Agente de Rede. Verifique também se as [portas usadas no Servidor de Administração](#) estão disponíveis.

3. No novo dispositivo, [instale o sistema de gerenciamento de banco de dados](#) (DBMS) que o Servidor de Administração usará.

Ao selecionar um DBMS, considere o número de dispositivos cobertos pelo Servidor de Administração.

4. Instale o Servidor de Administração no novo dispositivo.

Observe que, se você mover o servidor de banco de dados para o novo dispositivo, especifique o endereço local como o endereço IP do dispositivo no qual o banco de dados está instalado (o item "h" das instruções de [Instalação do Kaspersky Security Center](#)). Se precisar manter o servidor de banco de dados no dispositivo anterior, digite o endereço IP do dispositivo anterior no item "h" das instruções de [Instalação do Kaspersky Security Center](#).

5. Após a conclusão da instalação, recupere os dados do Servidor de Administração no novo dispositivo usando o [utilitário klbackup](#).

Se usar o SQL Server como um DBMS nos dispositivos anteriores e novos, observe que a versão do SQL Server instalada no novo dispositivo deverá ser igual ou posterior à versão do SQL Server instalada no dispositivo anterior. Caso contrário, não será possível recuperar os dados do Servidor de Administração no novo dispositivo.

6. Abra o Kaspersky Security Center 14 Web Console e [conecte-se ao Servidor de Administração](#).

7. Verifique se todos os dispositivos clientes estão conectados ao Servidor de Administração.

8. Desinstale o Servidor de Administração e o servidor de banco de dados do dispositivo anterior.

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. Na janela principal do aplicativo, clique no ícone **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. O Servidor de Administração virtual gerenciará os dispositivos do grupo selecionado (incluindo os subgrupos).

4. Na linha de menu, clique em **Novo Servidor de Administração virtual**.

5. Na página que se abre, defina as propriedades do novo Servidor de Administração virtual:

- **Nome do Servidor de Administração virtual.**

- **Endereço de conexão do Servidor de Administração**

É possível especificar o nome ou o endereço IP do Servidor de Administração.

6. Na lista de usuários, selecione o administrador do Servidor de Administração virtual. Se quiser, você poderá editar uma das contas existentes antes de atribuir a ela a função de administrador ou criar uma nova conta de usuário.

7. Clique em **Salvar**.

O novo Servidor de Administração virtual é criado, adicionado ao grupo de administração e exibido na guia **Servidores de Administração**.

Se você estiver conectado ao seu Servidor de Administração principal no Kaspersky Security Center 14 Web Console e não puder se conectar a um Servidor de Administração virtual gerenciado por um Servidor de Administração secundário, poderá usar uma das seguintes formas:

- [Modifique a instalação existente do Kaspersky Security Center 14 Web Console para adicionar o Servidor secundário à lista de Servidores de Administração confiáveis](#) . Em seguida, você poderá se conectar ao Servidor de Administração virtual no Kaspersky Security Center 14 Web Console.

1. No dispositivo em que o Kaspersky Security Center 14 Web Console está instalado, execute o arquivo de instalação `ksc-web-console-<número da versão>.<número da compilação>.exe` em uma conta com direitos administrativos.

2. O Assistente de Instalação será iniciado.

3. Na primeira página do Assistente, selecione a opção **Atualizar**.

4. Na página **Tipo de modificação**, selecione a opção **Editar as configurações de conexão**.

5. Na página **Servidores de Administração confiáveis**, adicione o Servidor de Administração secundário necessário.

6. Na última página do Assistente, clique em **Modificar** para aplicar as novas configurações.

7. Após a conclusão com êxito da reconfiguração do aplicativo, clique no botão **Concluir**.

- Use o Kaspersky Security Center 14 Web Console para [conectar-se diretamente ao Servidor de Administração secundário](#) em que o servidor virtual foi criado. Em seguida, você poderá trocar o Servidor de Administração virtual no Kaspersky Security Center 14 Web Console.
- Use o Console de Administração baseado em MMC para conectar-se diretamente ao Servidor virtual.

Uma hierarquia de Servidores de Administração

Um MSP pode executar múltiplos Servidores de Administração. Pode ser inconveniente administrar diversos Servidores de Administração separados, portanto uma hierarquia pode ser aplicada.

Em uma hierarquia, o Servidor de Administração Linux do Kaspersky Security Center só pode funcionar como um servidor secundário gerenciado por um Servidor de Administração principal do Kaspersky Security Center baseado em Windows ou do Kaspersky Security Center Cloud Console.

Uma configuração de "principal / secundário" para dois Servidores de Administração fornece as seguintes opções:

- Um Servidor de Administração secundário herda as políticas e tarefas do Servidor de Administração principal, prevenindo assim a duplicação das configurações.
- As seleções de dispositivos no Servidor de Administração principal podem incluir dispositivos de Servidores de Administração secundários.
- Os Relatórios no Servidor de Administração principal podem conter dados (incluindo informações detalhadas) de Servidores de Administração secundários.


Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de Administração secundário

Em uma hierarquia, o Servidor de Administração Linux do Kaspersky Security Center só pode funcionar como um servidor secundário gerenciado por um Servidor de Administração principal do Kaspersky Security Center baseado em Windows ou do Kaspersky Security Center Cloud Console.

Adição de Servidor de Administração secundário (executada no futuro Servidor de Administração principal)

Você pode adicionar um Servidor de Administração como um Servidor de Administração secundário, portanto, estabelecendo uma hierarquia "principal/secundário".

Para adicionar um Servidor de Administração secundário que está disponível para conexão por meio do Kaspersky Security Center 14 Web Console:

1. Assegure-se de que a porta 13000 do Servidor de Administração principal futuro esteja disponível para o recebimento de conexões de Servidores de Administração secundário.
2. No futuro Servidor de Administração principal, clique no ícone de **Configurações** .
3. Na página de propriedades que se abre, clique na guia **Servidores de Administração**.
4. Selecionar a caixa de seleção ao lado do nome do grupo de administração ao qual deseja adicionar o Servidor de Administração.
5. Na linha de menu, clique em **Conectar Servidor de Administração secundário**.
O Assistente de conectar Servidor de Administração secundário é iniciado.
6. 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.

- [Porta SSL do Servidor de Administração](#) [?]

Especifique o número da porta SSL no Servidor de Administração principal. O número da porta padrão é 13000.

- [Porta API do Servidor de Administração](#) [?]

Especifique o número da porta no Servidor de Administração principal para receber conexões através do OpenAPI. O número da porta padrão é 13299.

- [Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ](#) [?]

Selecione esta opção se o Servidor de Administração secundário estiver em uma zona desmilitarizada (DMZ).

Caso esta opção seja selecionada, o Servidor de Administração principal inicia a conexão com o Servidor de Administração secundário. Caso contrário, o Servidor de Administração secundário inicia a conexão com o Servidor de Administração principal.

- [Usar o servidor proxy](#) [?]

Selecione esta opção se você usar um servidor proxy para se conectar ao Servidor de Administração secundário.

Nesta caixa, é preciso também especificar as seguintes configurações do servidor proxy:

- **Endereço**
- **Nome do usuário**
- **Senha**

7. Siga as instruções do Assistente.

Após a conclusão do Assistente, a hierarquia "principal/secundário" é criada. A conexão entre os Servidores de Administração principal e secundário é estabelecida 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.

Adição de Servidor de Administração secundário (executada no futuro Servidor de Administração principal)

Se não conseguir se conectar ao futuro Servidor de Administração secundário (por exemplo, porque estava temporariamente desconectado ou indisponível), você ainda poderá adicionar um Servidor de Administração secundário.

Para adicionar como secundário um Servidor de Administração que não está disponível para a conexão através do Kaspersky Security Center 14 Web Console:

1. Envie o arquivo de certificado do futuro Servidor de Administração principal para o administrador de sistema do escritório onde o futuro Servidor de Administração secundário está localizado. (Você, por exemplo, pode gravar o arquivo em um dispositivo externo, como um pen drive, ou enviá-lo por e-mail.)

O arquivo de certificado está localizado no futuro servidor de Administração principal, em /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Solicita que administrador de sistema responsável pelo futuro Servidor de Administração secundário faça o seguinte:

a. Clique no ícone **Configurações** .

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. No campo **Endereço do Servidor de Administração Principal**, insira o nome da rede do Servidor de Administração principal futuro.

e. Selecione o arquivo com o certificado do Servidor de Administração principal futuro anteriormente salvo ao clicar em **Procurar**.

f. Se necessário, marque a caixa de seleção **Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ**.


g. Caso a conexão ao futuro servidor de administração secundário seja executada por meio de um servidor proxy, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão.

h. Clique em **Salvar**.

A hierarquia "principal/secundário" é construída. O Servidor de Administração principal começa a receber a conexão do Servidor de Administração secundário usando a 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.

Visualizar a lista de Servidores de administração secundários

Para visualizar a lista de Servidores de administração secundários (incluindo virtuais):

Na janela do aplicativo principal, clique no nome do Servidor de Administração, que está ao lado do ícone **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.

Os grupos de administração também são exibidos, mas estão em cinza e indisponíveis para gerenciamento neste menu.

Se você estiver conectado ao seu Servidor de Administração principal no Kaspersky Security Center 14 Web Console e não puder se conectar a um Servidor de Administração virtual gerenciado por um Servidor de Administração secundário, poderá usar uma das seguintes formas:

- [Modifique a instalação existente do Kaspersky Security Center 14 Web Console para adicionar o Servidor secundário à lista de Servidores de Administração confiáveis](#) . Em seguida, você poderá se conectar ao Servidor de Administração virtual no Kaspersky Security Center 14 Web Console.

1. No dispositivo em que o Kaspersky Security Center 14 Web Console está instalado, execute o arquivo de instalação `ksc-web-console-<número da versão>.<número da compilação>.exe` em uma conta com direitos administrativos.
2. O Assistente de Instalação será iniciado.
3. Na primeira página do Assistente, selecione a opção **Atualizar**.
4. Na página **Tipo de modificação**, selecione a opção **Editar as configurações de conexão**.
5. Na página **Servidores de Administração confiáveis**, adicione o Servidor de Administração secundário necessário.
6. Na última página do Assistente, clique em **Modificar** para aplicar as novas configurações.
7. Após a conclusão com êxito da reconfiguração do aplicativo, clique no botão **Concluir**.

- Use o Kaspersky Security Center 14 Web Console para [conectar-se diretamente ao Servidor de Administração secundário](#) em que o servidor virtual foi criado. Em seguida, você poderá trocar o Servidor de Administração virtual no Kaspersky Security Center 14 Web Console.
- Use o Console de Administração baseado em MMC para conectar-se diretamente ao Servidor virtual.

Ativando a proteção da conta contra modificações não autorizadas

Você pode ativar uma opção adicional para proteger uma conta de usuário contra modificações não autorizadas. Se essa opção for ativada, a modificação das configurações da conta do usuário requer autorização do usuário com direitos para modificação.

Para ativar ou desativar a proteção da conta contra modificações não autorizadas:

1. Acesse **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**.
2. Clique no nome da conta de usuário interno para a qual você deseja especificar a proteção da conta contra modificações não autorizadas.
3. Na janela aberta de configurações do usuário, clique na guia **Segurança de autenticação**.
4. Na guia **Segurança de autenticação**, selecione a opção **Solicitar autenticação para verificar permissão para modificar contas de usuário** se quiser solicitar credenciais sempre que as configurações de conta forem alteradas ou modificadas. Caso contrário, selecione a opção **Permitir que os usuários modifiquem esta conta sem autenticação adicional**.
5. Clique no botão **Salvar**.

Verificação em duas etapas

Esta seção descreve como você pode usar a verificação em duas etapas para reduzir o risco de acesso não autorizado ao Kaspersky Security Center 14 Web Console.

Cenário: configurando a verificação em duas etapas para todos os usuários

Este cenário descreve como ativar a verificação em duas etapas para todos os usuários e como excluir contas de usuário da verificação em duas etapas. Se você não ativou a verificação em duas etapas para sua conta antes de ativá-la para outros usuários, o aplicativo abre a janela para ativando a verificação em duas etapas para sua própria conta, primeiro. Este cenário também descreve como ativar a verificação em duas etapas para a sua própria conta.

Se você ativou a verificação em duas etapas para sua conta, pode prosseguir para a ativação da verificação em duas etapas para todos os usuários.

Pré-requisitos

Antes de começar:

- Certifique-se de que sua conta de usuário tenha o direito de Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões de usuário** para modificar as configurações de segurança para contas de outros usuários.
- Certifique-se de que os outros usuários do Servidor de Administração instalem um aplicativo autenticador em seus dispositivos.

Fases

Ativar a verificação em duas etapas para todos os usuários é feita com os seguintes passos:

1 Instalando um aplicativo autenticador em um dispositivo

Você pode instalar o Google Authenticator, Microsoft Authenticator ou qualquer outro aplicativo autenticador compatível com o algoritmo de senha única baseada em tempo.

2 Sincronizando a hora do aplicativo do autenticador com a hora do dispositivo no qual o Servidor de Administração está instalado

Certifique-se de que a hora definida no aplicativo autenticador está sincronizada com a hora do Servidor de Administração.

3 Ativando a verificação em duas etapas para sua conta e recebendo a chave secreta para sua conta

Após [ativar a verificação em duas etapas para a conta](#), é possível fazer a verificação em duas etapas para todos os usuários.

4 Ativando a verificação em duas etapas para todos os usuários

Os usuários [com a verificação em duas etapas ativada](#) devem usá-la para fazer login no servidor de administração.

5 Editando o nome de um emissor do código de segurança

Caso o usuário tenha vários servidores de administração com nomes semelhantes, [pode ser necessário alterar os nomes do emissor do código de segurança](#) para uma melhor identificação de diferentes servidores de administração.

6 Excluindo contas de usuário para as quais você não precisa ativar a verificação em duas etapas

Caso necessário, [exclua os usuários da verificação em duas etapas](#). Os usuários com contas excluídas não precisam usar a verificação em duas etapas para fazer login no Servidor de Administração.

Resultados

Após a conclusão deste cenário:

- A verificação em duas etapas está ativada para a sua conta.
- A verificação em duas etapas é ativada para todas as contas de usuário do Servidor de Administração, exceto para contas de usuário excluídas.

Sobre a verificação em duas etapas para uma conta

O Kaspersky Security Center Linux fornece verificação em duas etapas para usuários do Kaspersky Security Center 14 Web Console. Quando a verificação em duas etapas é ativada para a sua própria conta, toda vez que você efetua login no Kaspersky Security Center 14 Web Console, deve inserir seu nome de usuário, senha e um código de segurança único adicional. Para receber um código de segurança de uso único, você deve ter um aplicativo autenticador em seu computador ou dispositivo móvel.

Um código de segurança possui um identificador conhecido como *nome do emissor*. O nome do emissor do código de segurança é usado como um identificador do Servidor de Administração no aplicativo autenticador. Você pode alterar o nome do emissor do código de segurança. O nome do emissor do código de segurança possui um valor padrão que é igual ao nome do Servidor de Administração. O nome do emissor é usado como um identificador do Servidor de Administração no aplicativo autenticador. Se você alterar o nome do emissor do código de segurança, deverá emitir uma nova chave secreta e passá-la para o aplicativo autenticador. Um código de segurança é de uso único e válido por até 90 segundos (o tempo exato pode variar).

Qualquer usuário para o qual a verificação em duas etapas está ativada pode reemitir sua própria chave de segurança. Quando um usuário se autentica com a chave secreta reemitida e a usa para fazer login, o Servidor de Administração salva a nova chave secreta para a conta desse usuário. Se o usuário inserir a nova chave secreta incorretamente, o Servidor de Administração não salvará a nova chave secreta e deixará a chave secreta atual válida para autenticação posterior.

Qualquer software de autenticação compatível com o algoritmo de senha única com base em tempo (TOTP) pode ser usado como um aplicativo autenticador, por exemplo, o Google Authenticator. Para gerar o código de segurança, você deve sincronizar a hora definida no aplicativo do autenticador com a hora definida para o Servidor de Administração.

Um aplicativo autenticador gera o código de segurança da seguinte maneira:

1. O Servidor de Administração gera uma chave secreta especial e um código QR.
2. Você passa a chave secreta gerada ou o código QR para o aplicativo autenticador.

3. O aplicativo autenticador gera um código de segurança de uso único que você passa para a janela de autenticação do Servidor de Administração.

Recomendamos fortemente que você instale um aplicativo autenticador em um ou mais dispositivos. Salve a chave secreta (ou código QR) e mantenha-a em um lugar seguro. Isso ajudará a restaurar o acesso ao Kaspersky Security Center 14 Web Console, caso você perca o dispositivo móvel.

Para proteger o uso do Kaspersky Security Center, você pode ativar a verificação em duas etapas para sua própria conta e depois ativá-la para todos os usuários.

Você pode [excluir](#) contas da verificação em duas etapas. Isso pode ser necessário para contas de serviço que não podem receber um código de segurança para autenticação.

A verificação em duas etapas funciona de acordo com as seguintes regras:

- Apenas uma conta de usuário que tenha o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões do usuário** pode ativar a verificação em duas etapas para todos os usuários.
- Apenas um usuário que ativou a verificação em duas etapas para sua própria conta pode ativá-la para todos os usuários.
- Apenas um usuário que ativou a verificação em duas etapas para sua própria conta pode excluí-la da lista de verificação em duas etapas para todos os usuários.
- Um usuário pode ativar a verificação em duas etapas somente para a sua própria conta.
- Uma conta de usuário que possui o direito de Modificar ACLs de objetos na área funcional **Recursos gerais: Permissões do usuário** e está conectada ao Kaspersky Security Center 14 Web Console usando a verificação em duas etapas pode desativar a verificação em duas etapas: para qualquer outro usuário apenas se esse recurso estiver desativado, para um usuário excluído da lista de verificação em duas etapas que está ativado para todos os usuários.
- Qualquer usuário que efetuar login no Kaspersky Security Center 14 Web Console usando a verificação em duas etapas pode reemitir a chave secreta.
- Você pode ativar a opção de verificação em duas etapas para todos os usuários para o Servidor de Administração com o qual está trabalhando no momento. Se você ativar esta opção no Servidor de Administração, também ativará esta opção para as contas de usuário de seus Servidores de Administração virtuais e não ativará a verificação em duas etapas para as contas de usuário dos Servidores de Administração secundários.

Caso a verificação em duas etapas esteja ativada para uma conta de usuário no Servidor de Administração do Kaspersky Security Center versão 13 ou superior, o usuário não poderá fazer login no Kaspersky Security Center Web Console das versões 12, 12.1 ou 12.2.

Ativando a verificação em duas etapas para sua própria conta

Nesta etapa, você pode ativar a verificação em duas etapas apenas para sua própria conta.

Antes de começar a ativar a verificação em duas etapas para a sua conta, certifique-se de que um aplicativo autenticador esteja instalado no seu dispositivo móvel. Certifique-se de que a hora definida no aplicativo autenticador esteja sincronizada com a hora definida do dispositivo no qual o Servidor de Administração está instalado.

Para ativar a verificação em duas etapas para uma conta de usuário:

1. Acesse **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**.
2. Clique no nome da sua conta.
3. Na janela aberta de configurações do usuário, clique na guia **Proteção da conta**.
4. Na guia **Proteção da conta**:
 - Selecione a opção **Solicitar nome de usuário, senha e código de segurança (verificação em duas etapas)** se deseja ativar a verificação em duas etapas para uma conta de usuário:
 - Na janela aberta de verificação em duas etapas, insira a chave secreta no aplicativo autenticador ou escaneie o código QR para receber o código de segurança único.
Você pode especificar a chave secreta no aplicativo autenticador manualmente ou escanear o código QR no dispositivo móvel.
 - Na janela de verificação em duas etapas, especifique o código de segurança gerado pelo aplicativo autenticador e clique no botão **Verificar e aplicar**.
5. Clique no botão **Salvar**.

A verificação em duas etapas está ativada para a sua conta.

Ativando a verificação em duas etapas para todos os usuários

Você pode ativar a verificação em duas etapas para todos os usuários do Servidor de Administração se sua conta tiver o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões do usuário** e se você fizer a autenticação usando a verificação em duas etapas. Se você não ativou a verificação em duas etapas para sua conta antes de ativá-la para todos os usuários, o aplicativo abre a janela para [ativando a verificação em duas etapas para sua própria conta](#).

Para ativar a verificação em duas etapas para vários usuários:

1. Na janela principal do aplicativo, clique no ícone **Configurações** (⚙️) ao lado do nome do Servidor de Administração necessário.
A janela Propriedades do Servidor de Administração é aberta.
2. Na guia **Segurança de autenticação** da janela de propriedades, mude o botão seletor da opção de **verificação em duas etapas para todos os usuários** para a posição ativada.

A verificação em duas etapas está ativada para todos os usuários. A partir de agora, os usuários do Servidor de Administração, incluindo os usuários que foram adicionados após ativar a verificação em duas etapas para todos os usuários, devem configurar a verificação em duas etapas para suas contas, exceto os usuários **excluídos** do processo.

Desativando a verificação em duas etapas para uma conta de usuário

Você pode desativar a verificação em duas etapas para sua própria conta, bem como para contas de quaisquer outros usuários.

Você pode desativar a verificação em duas etapas da conta de outro usuário se sua conta tiver o direito de Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões do usuário**.

Para desativar a verificação em duas etapas para uma conta de usuário:

1. Acesse **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**.
2. Clique no nome da conta de usuário interna para a qual deseja desativar a verificação em duas etapas. Esta pode ser sua própria conta ou a de qualquer outro usuário.
3. Na janela aberta de configurações do usuário, clique na guia **Proteção da conta**.
4. Na guia **Proteção da conta**, selecione a opção **Solicitar apenas nome de usuário e senha** se deseja desativar a verificação em duas etapas para uma conta de usuário.
5. Clique no botão **Salvar**.

A verificação em duas etapas é desativada para a conta do usuário.

Desativando a verificação em duas etapas para todos os usuários

Você pode desativar a verificação em duas etapas para todos os usuários se o recurso estiver ativado para sua conta e você tiver o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões de usuário**. Se a verificação em duas etapas não estiver ativada, você deve [ativar a verificação em duas etapas para a sua conta](#) antes de desativá-la para todos os usuários.

Para desativar a verificação em duas etapas:

1. Na janela principal do aplicativo, clique no ícone **Configurações** (⚙️) ao lado do nome do Servidor de Administração necessário.
A janela Propriedades do Servidor de Administração é aberta.
2. Na guia **Segurança de autenticação** da janela de propriedades, mude o botão seletor da opção **verificação em duas etapas para todos os usuários** para a posição desativada.
3. Insira as credenciais da sua conta na janela de autenticação.

A verificação em duas etapas está desativada para todos os usuários.

Excluindo contas da verificação em duas etapas

Você pode excluir contas de usuário da verificação em duas etapas se tiver o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões de usuário**.

Se uma conta de usuário for excluída da lista de verificação em duas etapas para todos os usuários, esse usuário não precisará usar a verificação em duas etapas.

A exclusão de contas da verificação em duas etapas pode ser necessária para contas de serviço que não podem passar o código de segurança durante a autenticação.

Se deseja excluir algumas contas de usuário da verificação em duas etapas:

1. Na janela principal do aplicativo, clique no ícone **Configurações** (⚙️) ao lado do nome do Servidor de Administração necessário.

A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Segurança de autenticação** da janela de propriedades, na tabela de exclusões da verificação em duas etapas, clique no botão **Adicionar**.

3. Na janela aberta:

a. selecione as contas de usuário que deseja exportar.

b. Clique no botão **OK**.

As contas de usuário selecionadas são excluídas da verificação em duas etapas.

Gerando uma nova chave secreta

Você pode gerar uma nova chave secreta para verificação em duas etapas para sua conta apenas tiver autorização para usar esse recurso.

Para gerar uma nova chave secreta para uma conta de usuário:

1. Acesse **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**.

2. Clique no nome da conta de usuário para a qual você deseja gerar uma nova chave secreta para a verificação em duas etapas.

3. Na janela aberta de configurações do usuário, clique na guia **Proteção da conta**.

4. Na guia **Proteção da conta**, clique no link **Gerar uma nova chave secreta**.

5. Na janela aberta de verificação em duas etapas, especifique uma nova chave de segurança gerada pelo aplicativo autenticador.

6. Clique no botão **Verificar e aplicar**.

Uma nova chave secreta é gerada para o usuário.

Se o dispositivo móvel for perdido, será possível instalar um aplicativo autenticador em outro dispositivo móvel e gerar uma nova chave secreta para restaurar o acesso ao Kaspersky Security Center 14 Web Console.

Editando o nome de um emissor do código de segurança

Você pode ter várias tags (chamadas de emissores) para diferentes Servidores de Administração. Você pode alterar o nome de um emissor de código de segurança no caso, por exemplo, se o Servidor de Administração já usa um nome semelhante de emissor para outro Servidor de Administração. Por padrão, o nome de um emissor de código de segurança é igual ao nome do Servidor de Administração.

Depois de alterar o nome do emissor do código de segurança, você deve emitir novamente uma nova chave secreta e passá-la para o aplicativo autenticador.

Para especificar um novo nome de emissor do código de segurança:

1. Na janela principal do aplicativo, clique no ícone **Configurações** (⚙️) ao lado do nome do Servidor de Administração necessário.

A janela Propriedades do Servidor de Administração é aberta.

2. Na janela aberta de configurações do usuário, clique na guia **Proteção da conta**.

3. Na guia **Proteção da conta**, clique no link **Editar**.

A seção **Editar emissor do código de segurança** é aberta.

4. Especifique um novo nome de emissor do código de segurança.

5. Clique no botão **OK**.

Um novo nome de emissor de código de segurança é especificado para o Servidor de Administração.

Alterar o número permitido de tentativas de entrada de senha

O usuário do Kaspersky Security Center Linux pode inserir uma senha inválida um número limitado de vezes. Depois que o limite é atingido, a conta de usuário é bloqueada por uma hora.

Por padrão, o número máximo permitido de tentativas de entrada da senha é 10. Você pode alterar o número permitido de tentativas de entrada de senha, como descrito nesta seção.

Para alterar o número permitido de tentativas de entrada de senha:

1. No dispositivo do Servidor de Administração, execute uma linha de comando do Linux.

2. Para o utilitário `klscflag`, execute o seguinte comando:

```
sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSp1PpcLogonAttempts -t d -v N
```

onde N é o número de tentativas de inserir uma senha.

3. Para aplicar as alterações, reinicie o serviço do Servidor de Administração.

O número máximo de tentativas permitidas de entrada da senha é alterado.

Alterando credenciais de DBMS

Às vezes, pode ser necessário alterar as credenciais do DBMS, por exemplo, para realizar a rotatividade de credenciais para fins de segurança.

Para alterar as credenciais do DBMS em um ambiente Linux usando o utilitário klsrvconfig:


1. Inicie uma linha de comando do Linux.
2. Especifique o utilitário klsrvconfig na janela da linha de comando aberta:
`sudo /opt/kaspersky/ksc64/sbin/klsvconfig -set_dbms_cred`
3. Especifique um novo nome de conta. Você deve especificar as credenciais de uma conta que existe no DBMS.
4. Insira uma nova senha.
5. Especifique a nova senha para confirmação.

As credenciais do DBMS são alteradas.

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. Na parte superior da tela, clique no ícone **Configurações** , próximo ao 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 14 Web Console para exibir e ocultar seções e elementos da interface, dependendo dos recursos que estão sendo usados.

Para configurar a interface do Kaspersky Security Center 14 Web Console de acordo com o conjunto de recursos usados no momento:

1. Na janela principal do aplicativo, clique no menu da conta.
2. No menu suspenso, selecione **Opções da interface**.
3. Na janela **Opções da interface** exibida, ative ou desative as opções exigidas.
4. Clique em **Salvar**.

Depois disso, o console exibirá seções no menu principal de acordo com as opções habilitadas. Por exemplo, se você habilitar **Exibir alertas EDR**, a seção **MONITORAMENTO E RELATÓRIOS** → **ALERTAS** aparecerá no menu principal.

Localizar os dispositivos na rede

Esta seção descreve a pesquisa e a descoberta de dispositivos em rede.

O Kaspersky Security Center permite encontrar dispositivos com base em critérios especificados. Você pode salvar os resultados da pesquisa em um arquivo de texto.

O recurso de pesquisa e localização lhe permite localizar os seguintes dispositivos:

- Os dispositivos gerenciados nos grupos de administração do Servidor de Administração do Kaspersky Security Center e seus Servidores de Administração secundários.
- Dispositivos não atribuídos gerenciados por Servidor de Administração do Kaspersky Security Center e seus Servidores de Administração secundários.

Cenário: Localizar dispositivos na rede

Você deve executar a localização de dispositivos antes da instalação dos aplicativos de segurança. Quando todos os dispositivos em rede forem localizados, você pode receber informações sobre eles e gerenciá-los por meio de políticas. Sondagens de rede regulares são necessárias para saber se há algum novo dispositivo e se os dispositivos anteriormente localizados ainda estão na rede.

A localização de dispositivos na rede prossegue em estágios:

1 Descoberta de dispositivos inicial

Ao concluir o Assistente de Início Rápido, execute a descoberta de dispositivos manualmente.

2 Configuração de sondagens futuras

Certifique-se de que a [sondagem de conjunto de IPs](#) esteja ativada e de que o agendamento da amostragem atenda às necessidades da sua organização. Ao configurar o agendamento da sondagem, use as recomendações para a frequência de sondagem de rede.

Você também pode habilitar a [Sondagem Zeroconf](#) se sua rede incluir dispositivos IPv6.

3 Configuração de regras para adicionar dispositivos descobertos a grupos de administração (opcionais)

Se novos dispositivos aparecerem na sua rede, eles serão descobertos durante as sondagens 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 este estágio de configuração de regra, todos os dispositivos recentemente localizados 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.

Resultados

A conclusão do cenário produz o seguinte:

- O Servidor de Administração do Kaspersky Security Center Linux descobre os dispositivos que estão na rede e fornece informações sobre eles.

- As sondagens futuras são realizadas segundo o agendamento especificado.

Os dispositivos recentemente descobertos são organizados segundo as regras configuradas. (Ou, se nenhuma regra for configurada, os dispositivos permanecerão no grupo **Dispositivos não atribuídos**).

Sondagem do conjunto de IPs

O Kaspersky Security Center tenta executar a resolução de nome inversa para cada endereço IPv4 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. 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.

Inicialmente, o Kaspersky Security Center adquire conjuntos de IPs para amostragem a partir das configurações de rede do dispositivo no qual está instalado. Se o endereço de dispositivo for 192.168.0.1 e a máscara de sub-rede for 255.255.255.0, o Kaspersky Security Center incluirá a rede 192.168.0.0/24 na lista do endereço de amostragem automaticamente. O Kaspersky Security Center faz a amostragem de todos os endereços de 192.168.0.1 a 192.168.0.254.

Se apenas a sondagem de conjunto de IPs estiver habilitada, o Kaspersky Security Center descobrirá dispositivos apenas com endereços IPv4. Se sua rede incluir dispositivos IPv6, ative a [Sondagem Zeroconf](#) de dispositivos.

Visualização e modificação de configurações para amostragem de faixas IP

Para visualizar e modificar as propriedades para amostragem de faixas IP:

1. Acesse **DESCOBERTA E IMPLEMENTAÇÃO** → **DESCOBERTA** → **INTERVALOS de IPs**.
2. Clique no botão **Propriedades**.
A janela de propriedades da amostragem de faixas IP se abre.
3. Ative ou desative a amostragem de IP usando o botão de alternar **Permitir a sondagem**.
4. Configure o agendamento da amostragem. Por padrão, a amostragem de IP é executada a cada 420 minutos (sete horas).

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.

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 dias da semana](#) ?

A sondagem é executada regularmente, nos dias da semana e na hora especificados.

- [Todos os meses em dias especificados das semanas selecionadas](#) ?

A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

- [Executar tarefas ignoradas](#) ?

Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

Por padrão, esta opção está desativada.

5. Clique no botão **Salvar**.

As propriedades são salvas e aplicadas a todos os conjuntos de IPs.

Execução da amostragem manualmente

Para executar a amostragem imediatamente,

clique em **Iniciar sondagem**.

Adição e modificação de um conjunto de IPs

Inicialmente, o Kaspersky Security Center adquire conjuntos de IPs para amostragem a partir das configurações de rede do dispositivo no qual está instalado. Se o endereço de dispositivo for 192.168.0.1 e a máscara de sub-rede for 255.255.255.0, o Kaspersky Security Center incluirá a rede 192.168.0.0/24 na lista do endereço de amostragem automaticamente. O Kaspersky Security Center faz a amostragem 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.

Você pode criar um intervalo apenas para endereços IPv4. Se você ativar a [sondagem Zeroconf](#), o Kaspersky Security Center sondará toda a rede.

Para adicionar um novo conjunto de IPs:

1. Acesse **DESCOBERTA E IMPLEMENTAÇÃO** → **DESCOBERTA** → **INTERVALOS de IPs**.

2. Para adicionar um novo conjunto de IPs, clique no botão **Adicionar**.

3. Na janela que for aberta, especifique as seguintes configurações:

- **[Nome do intervalo IP](#)** 

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 também pode selecionar um dos conjuntos de IPs já existentes clicando no botão **Procurar**.

- **[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.

4. Selecione **Ativar sondagem de intervalos IP** se quiser fazer a amostragem da sub-rede ou do intervalo que adicionou. Caso contrário, a sub-rede ou o intervalo que você adicionou não serão amostrados.

5. Clique no botão **Salvar**.

O novo conjunto de IPs é adicionado à lista de conjuntos de IPs.

Você pode executar a amostragem de cada conjunto de IPs separadamente usando o botão **Iniciar sondagem**. 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.

Para adicionar uma sub-rede a um conjunto de IPs existente:

1. Acesse **DESCOBERTA E IMPLEMENTAÇÃO** → **DESCOBERTA** → **INTERVALOS de IPs**.

2. Clique no nome do conjunto de IPs ao qual deseja adicionar uma sub-rede.

3. Na janela que se abre, clique no botão **Adicionar**.

4. Especifique uma sub-rede usando o seu endereço e máscara ou usando o primeiro e o último endereço IP no conjunto de IPs. Ou adicione uma sub-rede existente clicando no botão **Procurar**.

5. Clique no botão **Salvar**.

A nova sub-rede é adicionada ao conjunto de IPs.

6. Clique no botão **Salvar**.

As novas configurações do conjunto de IPs são salvas.

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. Você pode ativar e desativar a amostragem independentemente para cada conjunto de IPs.

Sondagem Zeroconf

Este tipo de pesquisa é compatível apenas com pontos de distribuição baseados em Linux.

O Kaspersky Security Center pode sondar redes que possuem dispositivos com endereços IPv6. Nesse caso, os intervalos IP não são especificados e o Kaspersky Security Center sonda toda a rede usando a [rede zero configuração](#) (também chamada de *Zeroconf*). Para começar a usar o Zeroconf, você deve instalar o utilitário `avahi-browse` no dispositivo Linux que sonda as redes, o Servidor de Administração ou um ponto de distribuição.

Para habilitar a sondagem do Zeroconf:

1. Acesse **DESCOBERTA E IMPLEMENTAÇÃO** → **DESCOBERTA** → **INTERVALOS de IPs**.
2. Clique no botão **Propriedades**.
3. Na janela aberta, ative o botão **Usar Zeroconf para sondar redes IPv6**.

Em seguida, o Kaspersky Security Center começa a sondar a rede. Nesse caso, os intervalos IP especificados são ignorados.

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 permite-lhe *identificar* os dispositivos. Uma tag é um rótulo de um dispositivo que pode ser usado para agrupar, descrever ou encontrar 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 atribuição automática de tags é executada pelo Kaspersky Security Center 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, você pode definir uma regra que atribuirá o identificador [CentOS] a todos os dispositivos que executando o sistema operacional CentOS. Assim, é possível usar essa tag ao criar uma seleção de dispositivos. Isso ajudará a classificar todos os dispositivos CentOS 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 primário 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 **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 **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 **DISPOSITIVOS** → **TAGS** → **TAGS DE DISPOSITIVOS**.
2. Na lista, selecione o botão ao lado da tag do dispositivo que desejar 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.

Visualizando dispositivos aos quais uma tag está atribuída

Para visualizar dispositivos aos quais uma tag está atribuída:

1. No menu principal, vá para **DISPOSITIVOS** → **TAGS** → **TAGS DE DISPOSITIVOS**.
2. Clique no link **Visualizar dispositivos** ao lado da tag para a qual deseja visualizar os dispositivos atribuídos.
Se não vir o link **Visualizar dispositivos** ao lado de uma tag, isso indica que a tag não está atribuída a nenhum dispositivo.

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 **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.

Identificação de um dispositivo manualmente

Para atribuir uma tag a um dispositivo manualmente:

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.

Removendo uma tag atribuído de um dispositivo

Para remover uma tag de um dispositivo:

1. [Visualize as tags atribuídas ao dispositivo do qual deseja remover uma tag.](#)

2. Marque a caixa de seleção ao lado da tag que deseja remover.

3. Clique no botão **Desatribuir tag**.

4. Na janela que se abre, clique em **Sim**.

A tag é removida do dispositivo.

A tag de dispositivo não atribuída não é excluída. Se quiser, você poderá [excluí-lo manualmente](#).

Visualização de regras para identificar dispositivos automaticamente

Para visualizar regras para identificar dispositivos automaticamente,

Execute alguma das seguintes ações:

- No menu principal, vá para **DISPOSITIVOS** → **TAGS** → **REGRAS DE APLICAÇÃO AUTOMÁTICA DE TAGS**.
- No menu principal, vá para **DISPOSITIVOS** → **TAGS** 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, como o nome DNS do dispositivo ou a sua inclusão em um domínio ou em uma subrede IP.
- **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.
- **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](#)
- Após 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 respectivas 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](#).

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 Linux 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.

Implementação dos aplicativos Kaspersky

Esta seção descreve a implementação de aplicativos Kaspersky em dispositivos gerenciados, usando o Kaspersky Security Center 14 Web Console.

Cenário: Verificando a implementação dos aplicativos Kaspersky

Este cenário explica como implementar aplicativos Kaspersky por meio do Kaspersky Security Center 14 Web Console. Você pode usar o [Assistente de Início Rápido](#) e o Assistente de Implementação da Proteção ou concluir todas as etapas necessárias manualmente.

A implementação dos aplicativos da Kaspersky é feita em fases:

1 Download do plugin de gerenciamento da web para o aplicativo

[Baixe o plugin de gerenciamento da web para o Kaspersky Endpoint Security para Linux](#) no site da Kaspersky e, em seguida, [adicione o plugin do Kaspersky Security Center 14 Web Console](#).

2 Baixando e criando pacotes de instalação para aplicativos Kaspersky

[Baixe o pacote de distribuição do Agente de Rede](#) do site da Kaspersky e [crie um pacote de instalação do Agente de Rede](#).

Você pode usar o pacote de distribuição baixado para instalar o Agente de Rede localmente. Para fazer isso, siga as instruções fornecidas na [documentação do Kaspersky Endpoint Security for Linux](#).

3 Baixando e criando pacotes de instalação para o Kaspersky Endpoint Security for Linux

[Baixe o pacote de distribuição do Kaspersky Endpoint Security para Linux](#) no site da Kaspersky e [crie um pacote de instalação do Kaspersky Endpoint Security para Linux](#).

4 Criando um pacote de instalação independente (opcional)

Se você não conseguir instalar os aplicativos Kaspersky através do Kaspersky Security Center Linux em alguns dispositivos, por exemplo, em dispositivos de funcionários remotos, poderá [criar pacotes de instalação independentes](#) para aplicativos. Se você usar pacotes independentes para instalar aplicativos Kaspersky, as fases 5 e 6 abaixo podem ser desconsideradas.

5 Criação, configuração e execução da tarefa de instalação remota

Esta etapa faz parte do Assistente de Implementação da Proteção. Se optar por não executar o Assistente de Implementação da Proteção, [você deverá criar essa tarefa manualmente](#) e configurá-la manualmente.

Você também pode criar manualmente várias tarefas de instalação remotas para grupos de administração ou seleções de dispositivos diferentes. Você pode implementar versões diferentes de um aplicativo nessas tarefas.

Certifique-se de que todos os dispositivos na sua rede sejam descobertos; e execute a(s) tarefa(s) de instalação remotas.

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.

6 Criação e configuração de tarefas

A tarefa de *Atualizar* do Kaspersky Endpoint Security for Linux deve ser configurada.

Essa etapa faz parte do Assistente de Início Rápido: a tarefa é criada e configurada automaticamente com as configurações padrão. Se não tiver executado o Assistente, [você deverá criar essa tarefa manualmente](#) e configurá-la manualmente. Se você usar o Assistente de Início Rápido, certifique-se de que [a programação da tarefa](#) atenda aos seus requisitos. (Por padrão, o início agendado da tarefa está definido como **Manualmente**, mas você pode selecionar outra opção.)

7 Criar políticas

Crie a política do Kaspersky Endpoint Security para Linux [manualmente](#) ou por meio do Assistente de Início Rápido. Você pode usar as configurações padrão da política; pode também [modificar as configurações padrão](#) da política segundo as suas necessidades a qualquer momento.

8 Verificar os resultados

Certifique-se de que a implementação tenha sido concluída com sucesso: você tem políticas e tarefas para cada aplicativo, e esses aplicativos são instalados nos dispositivos gerenciados.

Resultados

A conclusão do cenário produz o seguinte:

- Todas as políticas e tarefas necessárias dos aplicativos selecionados são criadas.
- As programações de tarefas são configuradas segundo as suas necessidades.
- Os aplicativos selecionados são implementados ou planejados para ser implementados nos dispositivos cliente selecionados.

Adicionando plugins de gerenciamento para aplicativos Kaspersky

Para implementar um aplicativo Kaspersky, como o Kaspersky Endpoint Security for Linux, você deve baixar o plugin da web de gerenciamento de aplicativos.

Para baixar um plugin de gerenciamento para um aplicativo da Kaspersky:

1. [Baixe o plugin de gerenciamento da Web para Kaspersky Endpoint Security para Linux](#) no site da Kaspersky.
2. Abra o Kaspersky Security Center 14 Web Console.
3. Na lista suspensa **Configurações do console**, selecione **Plugins da web**.
Uma lista de plugins de gerenciamento disponíveis é exibida.
4. Clique no botão **Adicionar do arquivo**.
A janela **Adicionar do arquivo** é exibida.
5. Clique no botão **Carregar arquivo ZIP**.
6. Especifique o arquivo ZIP baixado do plugin da web.
7. Clique no botão **Carregar assinatura**.
8. Especifique o arquivo TXT baixado da assinatura do plugin da web.

9. Clique no botão **Adicionar**.

O Kaspersky Security Center verifica os arquivos carregados, adiciona e instala o plugin da web.

10. Quando a instalação for concluída, clique em **OK**.

O plugin da web de gerenciamento é instalado com a configuração padrão e exibido na lista de plugins da web de gerenciamento.

Criando pacotes de instalação a partir de um arquivo

Você pode usar os pacotes de instalação personalizada para fazer o seguinte:

- Instalar qualquer aplicativo (como um editor de texto) em um dispositivo cliente, por exemplo, através de uma [tarefa](#).
- Para [criar um pacote de instalação independente](#).

Um pacote de instalação personalizada é uma pasta com um conjunto de arquivos. Uma fonte para criar um pacote de instalação personalizada é um *arquivo morto*. O arquivo de compactação contém um ou mais arquivos que devem ser incluídos no pacote de instalação personalizada.

Ao criar um pacote de instalação personalizado, é possível especificar parâmetros da linha de comandos, por exemplo, para instalar o aplicativo em modo silencioso.

Para criar um pacote de instalação personalizado:

1. Execute uma das seguintes ações:

- Acesse **DESCOBERTA E IMPLEMENTAÇÃO** → **IMPLEMENTAÇÃO E ATRIBUIÇÃO** → **PACOTES DE INSTALAÇÃO**.
- Acesse **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 Novo Pacote é iniciado. 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 e clique no botão **Procurar**.

5. Na janela aberta, escolha o arquivamento 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).

Upload de arquivo para o Servidor de Administração é iniciado.

6. Se você especificou um arquivo de um aplicativo Kaspersky, receber uma solicitação para ler e aceitar o [Contrato de Licença do Usuário Final](#) (EULA) para o aplicativo. Para continuar, você deve aceitar o EULA. Selecione a opção **Aceitar os termos e condições deste Contrato de Licença do Usuário Final** se você leu, compreendeu e aceito integralmente os termos do EULA.

Além disso, você receber uma solicitação para ler e aceitar a [Política de Privacidade](#). Para continuar, você deve aceitar a Política de Privacidade. Selecione a opção comando abaixo **Eu aceito a Política de Privacidade** somente se você entender e concordar que seus dados serão tratados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade.

7. Na próxima página do Assistente, selecione um arquivo (na lista de arquivos extraídos do arquivo de compactação escolhido) e especifique os parâmetros da 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. A especificação de parâmetros da linha de comando é opcional.

O processo para criar o pacote de instalação é iniciado.

O Assistente informa quando o processo é concluído.

Se o pacote de instalação não for criado, a mensagem apropriada será exibida.

8. Clique no botão **Concluir** para fechar o Assistente.

O pacote de instalação que você criou é baixado na subpasta Packages da [pasta compartilhada do Servidor de Administração](#). Após o download, o pacote de instalação aparece na lista de pacotes de instalação.

Na lista de pacotes de instalação disponíveis no Servidor de Administração, clicando no link com o nome de um pacote de instalação personalizado, você pode:

- Visualize as seguintes propriedades de um pacote de instalação:
 - **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.
 - **Sistema operacional.** Tipo do sistema operacional ao qual o pacote de instalação se destina.
 - **Criação.** Data de criação do pacote de instalação.
 - **Modificação.** Data de modificação do pacote de instalação.
 - **Tipo.** Tipo do pacote de instalação.
- Mude os parâmetros de linha de comando.

Criar pacote de instalação autônomo

Você e os usuários de dispositivos na sua organização podem usar pacotes de instalação independente para instalar os aplicativos no dispositivo manualmente.

Um pacote de instalação independente (Installer.exe) é um arquivo executável que você pode armazenar em um Servidor da Web ou na pasta compartilhada, enviar por e-mail ou transferir para um dispositivo cliente usando outro método. No dispositivo cliente, o usuário pode executar o arquivo recebido localmente para instalar um aplicativo sem envolver o Kaspersky Security Center Linux. Você pode criar pacotes de instalação independentes para aplicativos Kaspersky e de terceiros. Para criar um pacote de instalação independente para um aplicativo de terceiros, você deve [criar um pacote de instalação personalizado](#).

Verifique se o pacote de instalação independente não está disponível para terceiros.

Para criar um pacote de instalação independente:

1. Execute uma das seguintes ações:

- Acesse **DESCOBERTA E IMPLEMENTAÇÃO** → **IMPLEMENTAÇÃO E ATRIBUIÇÃO** → **PACOTES DE INSTALAÇÃO**.
- Acesse **OPERAÇÕES** → **REPOSITÓRIOS** → **PACOTES DE INSTALAÇÃO**.

Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Na lista de pacotes de instalação, selecione um pacote de instalação e, acima da lista, clique no botão **Implementar**.

3. 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**.

4. Na primeira página do Assistente, certifique-se de que 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.

5. Na página **Migrar para a lista de dispositivos gerenciados** do Assistente, selecione a opção **Não migrar dispositivos**. 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**.

6. Na próxima página do Assistente, quando o processo de criação do pacote de instalação independente for concluído, clique no botão **CONCLUIR**.

O Assistente de Criação de Pacote de Instalação Independente é fechado.

O pacote de instalação independente é criado e colocado na subpasta PkgInst da [pasta compartilhada do Servidor de Administração](#). Você pode visualizar a lista de pacotes independentes, clicando no botão **Exibir a lista de pacotes independentes** acima da lista de pacotes de instalação.

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:

Acima da lista, clique no botão **Exibir a lista de pacotes independentes**.

Na lista de pacotes de instalação independentes, as seguintes propriedades são exibidas:

- **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 aplicativo.** Nome do aplicativo incluído no pacote de instalação independente.
- **Versão do aplicativo.**
- **Nome do pacote de instalação do Agente de Rede.** A propriedade será exibida apenas se o Agente de Rede estiver incluído no pacote de instalação independente.
- **Versão do Agente de Rede.** A propriedade será exibida apenas se o Agente de Rede estiver incluído no pacote de instalação independente.
- **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.
- **Caminho.** Caminho completo para a pasta em que o pacote de instalação independente está localizado.
- **Endereço da Web.** Endereço da Web do local 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:

- Publique um pacote de instalação independente no servidor da Web, clicando no botão **Publicar**. O pacote de instalação independente publicado está disponível para download para usuários aos quais você enviou o link para o pacote de instalação independente.
- Anular publicação de um pacote de instalação independente no Servidor da Web clicando no botão **Cancelar a publicação**. O pacote de instalação independente não publicado está disponível para download apenas para você e outros administradores.
- Baixe um pacote de instalação independente para o seu dispositivo clicando no botão **Baixar**.
- Envie um e-mail com o link para um pacote de instalação independente clicando no botão **Enviar por e-mail**.
- Remova um pacote de instalação independente clicando no botão **Remover**.

Instalação de aplicativos usando a tarefa de instalação remota

O Kaspersky Security Center Linux permite instalar aplicativos em dispositivos remotamente, usando tarefas de instalação remotas. Essas tarefas são criadas e atribuídas aos dispositivos por um Assistente dedicado. Para atribuir uma tarefa aos dispositivos mais rapidamente e facilmente, você pode especificar os dispositivos na janela Assistente em uma das seguintes formas:

- **Selecionar os dispositivos na rede detectados pelo Servidor de Administração.** Neste caso, a tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.
- **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista.** Você pode especificar nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisa atribuir a tarefa.
- **Atribuir a tarefa a uma seleção de dispositivos.** Neste caso, a tarefa é atribuída aos dispositivos incluídos em uma seleção anteriormente criada. Você pode especificar a seleção padrão ou uma personalizada que você criou.
- **Atribuir tarefa a um grupo de administração.** Neste caso, a tarefa é atribuída aos dispositivos incluídos em um grupo de administração anteriormente criado.

Para o desempenho correto da instalação remota em um dispositivo cliente com o Agente de Rede instalado, as seguintes portas devem ser abertas: a) TCP 139 e 445; b) UDP 137 e 138. Por padrão, essas portas são abertas para todos os dispositivos incluídos no domínio. Elas são abertas automaticamente usando o utilitário de preparação de instalação remota.

Instalar um aplicativo nos dispositivos específicos

Esta seção contém informações sobre como instalar um aplicativo remotamente em um grupo de administração, dispositivos com endereços IP específicos ou uma seleção de dispositivos gerenciados.

Para instalar um aplicativo nos dispositivos específicos:

1. Estabeleça uma conexão com o Servidor de Administração que controle os dispositivos relevantes.

2. No menu principal, vá para **DISPOSITIVOS** → **TAREFAS**.

3. Clique em **Adicionar**.

O Assistente para Adicionar Tarefas é iniciado.

4. No campo **Tipo de tarefa**, selecione **Instalar o aplicativo remotamente**.

5. 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 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. Siga as instruções do Assistente.

O assistente para adição de tarefa cria uma tarefa para instalação remota do aplicativo selecionado no assistente em dispositivos específicos. Se você selecionou a opção **Atribuir tarefa a um grupo de administração**, a tarefa será de grupo.

7. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação que especificou nas configurações da tarefa.

Quando a tarefa de instalação remota for concluída, o aplicativo selecionado será instalado nos dispositivos específicos.

Instalar um aplicativo usando as políticas de grupo do Active Directory

O Kaspersky Security Center permite instalar os aplicativos Kaspersky em dispositivos gerenciados, usando as políticas de grupo do Active Directory.

Você pode instalar aplicativos usando as políticas de grupo do Active Directory apenas dos pacotes de instalação que incluam Agente de Rede.

Para instalar um aplicativo usando as políticas de grupo do Active Directory:

1. Execute o Assistente de Implementação da Proteção. Siga as instruções do Assistente.
2. Na página [Configurações da tarefa de instalação remota](#) do Assistente de Implementação da Proteção, habilite a opção **Atribuir a instalação do pacote em políticas de grupo do Active Directory**.
3. Na página [Selecionar contas para acessar os dispositivos](#), selecione a opção **Conta necessária (Agente de Rede não é usado)**.
4. Adicionar a conta com privilégios de administrador no dispositivo onde o Kaspersky Security Center é instalado ou na conta incluída no grupo de domínio Proprietários do criador de política de grupo.
5. Conceda as permissões para a conta selecionada:
 - a. Acesse **Painel de Controle** → **Ferramentas Administrativas** e abra **Gerenciamento de Política de Grupo**.
 - b. Clique no nó com o domínio desejado.
 - c. Clique na seção **Delegação**.
 - d. Na lista suspensa de **Permissão**, selecione **Vincular GPOs**.
 - e. Clique em **Adicionar**.
 - f. Na janela aberta **Selecionar usuário, computador ou grupo**, selecione a conta desejada.
 - g. Clique em **OK** para fechar a janela **Selecionar usuário, computador ou grupo**.
 - h. Na lista **Grupos e usuários**, selecione a conta recém-adicionada, depois clique em **Avançado** → **Avançado**.
 - i. Na lista **Entradas de permissão**, clique duas vezes na conta recém-adicionada.
 - j. Conceda as seguintes permissões:
 - **Criar objetos de grupo**
 - **Excluir objetos de grupo**
 - **Criar objetos de contêiner de política de grupo**
 - **Excluir objetos de contêiner de política de grupo**
 - k. Clique em **OK** para salvar as alterações.
6. Defina outras configurações seguindo as instruções do Assistente.
7. Execute manualmente a tarefa de instalação remota criada ou aguarde pelo seu início programado.

Isto inicia a seguinte sequência de instalação remota:

1. Quando a tarefa estiver em execução, os seguintes objetos são criados em cada domínio que inclui os quaisquer dispositivos cliente do conjunto especificado:
 - Objeto da política de grupo (GPO) sob o nome **Kaspersky_AK{GUID}**.
 - Um grupo de segurança que corresponde à GPO. Esse grupo de segurança inclui dispositivos cliente abrangidos pela tarefa. O conteúdo do grupo de segurança define o escopo da GPO.
2. O Kaspersky Security Center instala os aplicativos Kaspersky selecionados nos dispositivos cliente de Share, que é a pasta de rede compartilhada no aplicativo. Na pasta de instalação do Kaspersky Security Center, será criada uma pasta alojada auxiliar que contém o arquivo .msi para o aplicativo a ser instalado.
3. Quando novos dispositivos são adicionados ao escopo da tarefa, são adicionados ao grupo de segurança após o início da próxima tarefa. Se a opção **Executar tarefas perdidas** estiver selecionada no agendamento da tarefa, os dispositivos são adicionados imediatamente ao grupo de segurança.
4. Quando dispositivos são excluídos do escopo da tarefa, são excluídos também do grupo de segurança após o início da próxima tarefa.
5. Quando uma tarefa for excluída do Active Directory, a GPO, o link para o GPO e o grupo de segurança correspondente serão excluídos também.

Se quiser aplicar outro esquema de instalação usando o Active Directory, você pode definir as configurações necessárias manualmente. Por exemplo, isso poderá ser necessário nos seguintes casos:

- Quando o administrador da proteção de antivírus não tem direitos para efetuar alterações ao Active Directory de determinados domínios;
- Quando o pacote de instalação original tiver que ser armazenado em um recurso de rede separado;
- Quando é necessário vincular uma GPO a unidades específicas do Active Directory

Estão disponíveis as opções que se seguem para usar um esquema de instalação alternativo através do Active Directory:

- Se a instalação tiver que ser realizada diretamente da pasta compartilhada do Kaspersky Security Center, nas propriedades da GPO do Active Directory especifique o arquivo .msi localizado na subpasta de execução da pasta do pacote de instalação para obter o aplicativo desejado.
- Se o pacote de instalação tiver de ser localizado em outro recurso de rede, é necessário copiar a totalidade do conteúdo da pasta exec, já que além do arquivo com a extensão, a pasta contém arquivos de configuração gerados quando o pacote foi criado. Para instalar a chave de licença com o aplicativo, copie também o arquivo de chave para essa pasta.

Instalando aplicativos nos Servidores de Administração secundários

Para instalar um aplicativo em Servidores de Administração secundários:

1. Estabeleça uma conexão ao Servidor de Administração que controla os Servidores de Administração secundários relevantes.
2. Certifique-se de que o pacote de instalação corresponde ao aplicativo sendo instalado em cada um dos Servidores de Administração secundários selecionados. Se você não encontrar o pacote de instalação em

nenhum dos Servidores secundários, distribua-o. Para este efeito, [crie uma tarefa](#) com o tipo de tarefa **Distribuir pacote de instalação**.

3. [Crie uma tarefa para uma instalação de aplicativo remoto](#) em Servidores de Administração secundários. Selecione o tipo de tarefa **Instalar o aplicativo no Servidor de Administração secundário remotamente**.

O assistente para adição de tarefa cria uma tarefa para instalação remota do aplicativo selecionado no assistente em Servidores de Administração secundários específicos.

4. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação que especificou nas configurações da tarefa.

Quando a tarefa de instalação remota for concluída, o aplicativo selecionado será instalado nos Servidores de Administração secundários.

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 **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 14 Linux 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 14 Linux 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 14 Linux usa o diretório especificado como um diretório temporário para acessar o 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 da Kaspersky através do Kaspersky Security Center Linux pode necessitar a remoção de software de terceiros incompatível com o aplicativo sendo instalado. O Kaspersky Security Center 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 no Assistente de Implementação da Proteção. Quando esta opção está ativada, o Kaspersky Security Center remove aplicativos incompatíveis antes de instalar um aplicativo de segurança em um dispositivo gerenciado.

Instruções: [Removendo aplicativos incompatíveis antes da instalação](#)

Remover aplicativos incompatíveis através de uma tarefa dedicada

Para remover aplicativos incompatíveis, 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.

Instruções de como proceder: [Criação de uma tarefa](#)

Remover aplicativos ou atualizações de software remotamente

Você pode remover aplicativos ou atualizações de software em dispositivos gerenciados que executam o Linux remotamente apenas usando o Agente de Rede.

Para remover aplicativos ou atualizações de software remotamente de dispositivos selecionados:

1. Na janela principal do aplicativo, vá para **DISPOSITIVOS** → **TAREFAS**.
2. Clique em **Adicionar**.
O Assistente para Adicionar Tarefas é iniciado. Prossiga pelo Assistente usando o botão **Avançar**.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Desinstalar aplicativo remotamente**.
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 (* <>?:\|).
O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\|).
5. Selecione os dispositivos aos quais a tarefa será atribuída.

6. Selecione o tipo de software que deseja remover e, em seguida, selecione os aplicativos, atualizações ou patches específicos que deseja remover:

- [Desinstalar o aplicativo gerenciado](#) 

Uma lista de aplicativos da Kaspersky é exibida. Selecione o aplicativo que deseja remover.

- [Desinstalar aplicativo incompatível](#) 

Uma lista de aplicativos incompatíveis com os aplicativos de segurança da Kaspersky ou do Kaspersky Security Center é exibida. Marque as caixas de seleção ao lado dos aplicativos que deseja remover.

- [Desinstalar aplicativo do registro de aplicativos](#) 

Por padrão, os Agentes de Rede enviam ao Servidor de Administração informações sobre os aplicativos instalados nos dispositivos gerenciados. A lista de aplicativos instalados é armazenada no registro de aplicativos.

Para selecionar um aplicativo no registro de aplicativos:

- a. Clique no campo **Aplicativo a ser desinstalado** e selecione o aplicativo que deseja remover.
- b. Especifique as opções de desinstalação:

- [Modo de desinstalação](#) 

Selecione como deseja remover o aplicativo:

- **Definir o comando de desinstalação automaticamente**


Se o aplicativo tiver um comando de desinstalação definido pelo fornecedor do aplicativo, o Kaspersky Security Center usa esse comando. Recomendamos que você selecione esta opção.

- **Especificar o comando de desinstalação**

Selecione esta opção se desejar especificar seu próprio comando para a desinstalação do aplicativo.

Recomendamos que você primeiro tente remover o aplicativo usando a opção **Definir o comando de desinstalação automaticamente**. Se a desinstalação por meio do comando definido automaticamente falhar, use seu próprio comando.

Digite um comando de instalação no campo e especifique a seguinte opção:

[Use este comando para desinstalação apenas se o comando padrão não tiver sido autodetectado](#) 

O Kaspersky Security Center verifica se o aplicativo selecionado tem ou não um comando de desinstalação definido pelo fornecedor do aplicativo. Se o comando for encontrado, o Kaspersky Security Center o usará em vez do comando especificado no campo **Comando para desinstalação de aplicativos**.

Recomendamos que você ative esta opção.

- [Efetuar reinício após a desinstalação bem-sucedida do aplicativo](#) 

Se o aplicativo exigir que o sistema operacional seja reiniciado no dispositivo gerenciado após a desinstalação bem-sucedida, o sistema operacional será reiniciado automaticamente.

7. Especifique como os dispositivos clientes farão o download do utilitário de desinstalação:

- [Usando o Agente de Rede](#) 

Os arquivos são entregues aos dispositivos clientes pelo Agente de Rede instalado nesses dispositivos. Se esta opção estiver desativada, os arquivos serão entregues usando as ferramentas do sistema operacional Linux. Recomendamos que você ative esta opção se a tarefa tiver sido atribuída a dispositivos com o Agente de Rede instalado.

- [Usando recursos do sistema operacional através do Servidor de Administração](#) ⓘ

A opção está obsoleta. Em vez disso, use a opção **Usando o Agente de Rede** ou **Usando recursos do sistema operacional através de pontos de distribuição**.

Os arquivos são transmitidos para dispositivos clientes usando as ferramentas do sistema operacional do Servidor de Administração. Você pode ativar esta opção se nenhum Agente de Rede estiver instalado no dispositivo cliente, mas o dispositivo cliente está na mesma rede que o Servidor de Administração.

- [Usando recursos do sistema operacional através de pontos de distribuição](#) ⓘ

Os arquivos são transmitidos para dispositivos clientes usando ferramentas do sistema operacional por meio de pontos de distribuição. Você pode ativar esta opção se houver, no mínimo, um ponto de distribuição na rede.

Se a opção **Usando o Agente de Rede** estiver marcada, os arquivos serão entregues por meio das ferramentas do sistema operacional somente se os recursos do Agente de Rede estiverem indisponíveis.

- [Número máximo de downloads concomitantes](#) ⓘ

O número máximo permitido de dispositivos clientes para os quais o Servidor de Administração pode transmitir os arquivos simultaneamente. Quanto maior esse número, mais rápido o aplicativo será desinstalado, mas a carga no Servidor de Administração será maior.

- [Número máximo de tentativas de desinstalação](#) ⓘ

Se, ao executar a tarefa *Desinstalar aplicativo remotamente*, o Kaspersky Security Center falhar em desinstalar um aplicativo em um dispositivo gerenciado dentro do número de execuções do instalador especificado pelo parâmetro, o Kaspersky Security Center interromperá a entrega do pacote de desinstalação a este dispositivo gerenciado e não iniciará mais o instalador no dispositivo.

O parâmetro **Número máximo de tentativas de desinstalação** permite salvar os recursos do dispositivo gerenciado, assim como reduzir o tráfego (desinstalação, execução do arquivo MSI e mensagens de erro).

As tentativas recorrentes de início de tarefas podem indicar um problema no dispositivo e que impede a desinstalação. O administrador deve resolver o problema dentro do número especificado de tentativas de desinstalação e, em seguida, reiniciar a tarefa (manualmente ou por programação).

Se a desinstalação não for realizada eventualmente, o problema será considerado não solucionável e quaisquer tarefas adicionais serão consideradas como custosas em termos de consumo desnecessário de recursos e tráfego.

Quando a tarefa é criada, o contador de tentativas fica definido como 0. Cada execução do instalador retorna um erro no dispositivo e incrementa a leitura do contador.

Se o número de tentativas especificado no parâmetro tiver sido excedido e o dispositivo estiver pronto para a desinstalação do aplicativo, você poderá aumentar o valor do parâmetro **Número máximo de tentativas de desinstalação** e iniciar a tarefa para desinstalar o aplicativo. Alternativamente, você pode criar uma nova tarefa *Desinstalar aplicativo remotamente*.

- [Verificar o tipo do sistema operacional antes de baixar](#) ⓘ

Antes de transmitir os arquivos para dispositivos clientes, o Kaspersky Security Center verifica se as configurações do pacote de desinstalação são aplicáveis ao sistema operacional do dispositivo cliente. Se as configurações não forem aplicáveis, o Kaspersky Security Center não transmitirá os arquivos e não tentará desinstalar o aplicativo. Por exemplo, para desinstalar algum aplicativo de dispositivos de um grupo de administração que inclui dispositivos que executam vários sistemas operacionais, você pode atribuir a tarefa de desinstalação ao grupo de administração e então ativar esta opção para ignorar os dispositivos que executem um sistema operacional diferente do exigido.

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).

- [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. Se necessário, adicione as contas que serão usadas para iniciar a tarefa de desinstalação remota:

- [Nenhuma conta necessária \(Agente de Rede instalado\)](#)²

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 \(Agente de Rede não é usado\)](#)²

Se essa caixa de seleção estiver selecionada, você poderá especificar uma conta sob a qual o instalador do aplicativo será executado. Você poderá especificar a conta do usuário se o Agente de Rede não estiver instalado nos dispositivos para os quais a tarefa foi atribuída.

Você pode especificar múltiplas contas de usuário se, por exemplo, nenhuma delas tiver os direitos necessários em todos os dispositivos para os quais a tarefa foi atribuída. Nesse caso, todas as contas que foram adicionadas são usadas para executar a tarefa, por ordem consecutiva, de cima para baixo.

Se nenhuma conta for adicionada, a tarefa será executada na conta em que o serviço do Servidor de Administração está sendo executado.

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 Propriedades da tarefa, especifique as [configurações gerais da tarefa](#).

14. Clique no botão **Salvar**.

15. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação que você especificou nas configurações da tarefa.

Após a conclusão da tarefa de desinstalação remota, o aplicativo selecionado será removido dos dispositivos clientes selecionados.

Preparo de um dispositivo executando o SUSE Linux Enterprise Server 15 para instalação do agente de rede

Para instalar o agente de rede em um dispositivo com o sistema operacional SUSE Linux Enterprise Server 15:

Antes da instalação do agente de rede, execute o seguinte comando:

```
$ sudo zypper install insserv-compat
```

Isso permite a instalação do pacote `insserv-compat` e configure o agente de rede corretamente.

Execute o comando `rpm -q insserv-compat` para verificar se o pacote já está instalado.

Caso a rede inclua muitos dispositivos executando o SUSE Linux Enterprise Server 15, será possível usar o software especial para configurar e gerenciar a infraestrutura da empresa. Ao usar o software, é possível instalar automaticamente o pacote `insserv-compat` em todos os dispositivos necessários de uma só vez. Por exemplo, é possível usar Puppet, Ansible, Chef e ainda criar o próprio script. Use qualquer método conveniente para você.

Depois de preparar o dispositivo SUSE Linux Enterprise Server 15, [implante e instale o Agente de Rede](#).

Aplicativos Kaspersky: licenciamento e ativação

Esta seção descreve os recursos do Kaspersky Security Center relacionados ao trabalho com chaves de licença de aplicativos gerenciados da Kaspersky.

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

Ao adicionar uma chave de licença usando o Kaspersky Security Center, 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.

Licenciamento de aplicativos gerenciados

Os aplicativos Kaspersky instalados em dispositivos gerenciados devem ser licenciados com a aplicação de um arquivo de chave ou um código de ativação à cada um dos aplicativos. Um arquivo de licença ou um código de ativação pode ser implementado nas seguintes formas:

- Implementação automática
- O pacote de instalação de um aplicativo gerenciado
- A tarefa de adicionar uma chave de licença para um aplicativo gerenciado
- Ativação manual de um aplicativo gerenciado

É possível adicionar uma nova chave de licença ativa ou reserva por qualquer um dos métodos listados acima. Um aplicativo da Kaspersky usa uma chave ativa no momento e armazena uma chave reserva para aplicar após a expiração da chave ativa. 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.

Implementação automática

Se você usar aplicativos gerenciados diferentes e precisa implementar um arquivo de chave ou código de ativação específico para dispositivos, opte por outras formas de implementar aquele código de ativação ou arquivo de chave.

O Kaspersky Security Center lhe permite implementar automaticamente as chaves de licença disponíveis nos dispositivos. Por exemplo, três chaves de licença são armazenadas no repositório do Servidor de Administração. Você ativou a opção **Chave de licença automaticamente distribuída** para as três chaves de licença. Um aplicativo de segurança da Kaspersky — por exemplo, Kaspersky Endpoint Security for Linux — é instalado nos dispositivos da organização. Um novo dispositivo é descoberto, no qual uma chave de licença deve ser implementada. O aplicativo determina, por exemplo, que duas das chaves de licença do repositório podem ser implementadas ao dispositivo: a chave de licença denominada *Key_1* e chave de licença denominada *Key_2*. Uma destas chaves de licença é implementada no dispositivo. Neste caso, não pode ser previsto qual das duas chaves de licença será implementada no dispositivo, porque a implementação automática de chaves de licença não é fornecida para nenhuma atividade do administrador.

Quando uma chave de licença é implementada, os dispositivos são recontados para aquela chave de licença. Você deve assegurar-se de que o número de dispositivos nos quais a chave de licença foi implementada não excede o limite da licença. Se o [número de dispositivos exceder o limite de licença](#), todos os dispositivos que não foram cobertos pela licença serão terão o status *Crítico* atribuído.

Antes da implementação, o arquivo de chave ou o código de ativação deve ser adicionado ao repositório do Servidor de Administração.

Instruções de como proceder:

- [Adição de uma chave de licença ao repositório do Servidor de Administração](#)
- [Distribuição automática de uma chave de licença](#)

Adicionando um arquivo de chave ou código de ativação ao pacote de instalação de um aplicativo gerenciado

Por motivos de segurança, esta opção não é recomendada. Um arquivo de licença ou um código de ativação adicionado a um pacote de instalação pode se tornar comprometido.

Se você instalar um aplicativo gerenciado usando um pacote de instalação, poderá especificar um código de ativação ou um arquivo de chave neste pacote de instalação ou na política do aplicativo. A chave de licença será implementada nos dispositivos gerenciados no momento da próxima sincronização do dispositivo com o Servidor de Administração.

Instruções de uso: [Adicionando uma chave de licença a um pacote de instalação](#)

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

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

Antes da implementação, o arquivo de chave ou o código de ativação deve ser adicionado ao repositório do Servidor de Administração.

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.

Adição de uma chave de licença ao repositório 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. Selecione o que você quer adicionar:
 - **Adicionar arquivo de chave**
Clique no botão **Selecionar arquivo de chave** e navegue até o arquivo .key que deseja adicionar.
 - **Inserir código de ativação**
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 14 Web Console permite distribuir uma chave de licença para dispositivos cliente usando a tarefa *Distribuição de chaves de licença*.

Para distribuir uma chave de licença aos dispositivos cliente:

1. No menu principal, vá para **DISPOSITIVOS** → **TAREFAS**.
2. Clique em **Adicionar**.
O Assistente para Adicionar Tarefas é iniciado.
3. Selecione o aplicativo para o qual deseja adicionar uma chave de licença.
4. Do **Tipo de tarefa** lista, selecione **Adicionar chave de licença**.
5. Siga as instruções do Assistente.
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. Para executar a tarefa, selecione-a na lista de tarefas e clique no botão **Iniciar**.

Quando a tarefa for executada, a chave de licença será implementada nos dispositivos selecionados.

Distribuição automática de uma chave de licença

O Kaspersky Security Center Linux 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 abrir, selecione a caixa de seleção **Distribuir automaticamente a chave de licença nos 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.

Se a caixa de seleção **Distribuir automaticamente a chave de licença nos dispositivos gerenciados** for marcada na janela de propriedades da chave de licença, uma chave de licença é distribuída em sua rede imediatamente. Ao não selecionar essa opção, é possível distribuir uma chave de licença manualmente posteriormente.

Visualizando de informações sobre chaves de licença em uso

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 os arquivo de chave e os 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

Para exibir quais chaves de licença são implementadas em um dispositivo cliente específico:

1. No menu principal, vá para **DISPOSITIVOS** → **DISPOSITIVOS GERENCIADOS**.
2. Clique no nome do dispositivo necessário.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Aplicativos**.
4. Clique no nome do aplicativo do qual deseja exibir as informações sobre a chave de licença.
5. Na janela de propriedades do aplicativo que se abre, clique na guia **Geral** e abra a seção **Licença**.

As informações principais sobre as chaves de licença adicional ativas são exibidas.

Para definir configurações atualizadas das chaves de licença do Servidor de Administração virtual, o Servidor de Administração envia uma solicitação para os servidores de ativação da Kaspersky ao menos uma vez por dia.

Excluindo uma chave de licença do repositório

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

Para excluir um arquivo de chave ou um código de ativação do repositório do Servidor de Administração:

1. Acesse **OPERAÇÕES** → **LICENCIAMENTO** → **LICENÇAS DA KASPERSKY**.
2. Selecione o arquivo de chave ou o código de ativação que deseja excluir do repositório.
3. Clique no botão **Excluir**.
4. Confirmar a operação clicando no botão **OK**.

O arquivo de chave ou o código de ativação selecionado são excluídos do repositório.

Você pode [adicionar](#) novamente uma chave de licença excluída ou adicionar uma nova chave de licença.

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. É necessário desinstalar o aplicativo selecionado antes de revogar seu EULA.

Para revogar o EULA dos aplicativos gerenciados da Kaspersky:

1. Abra a janela de propriedades do Servidor de Administração e na guia **Geral**, selecione a seção **Contratos de Licença do Usuário Final**.

É exibida uma lista de EULAs, aceitos ao criar pacotes de instalação, durante a instalação contínua de atualizações ou mediante implementação do Kaspersky Security for Mobile.

2. 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

3. 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, aplicativos móveis) vinculados ao EULA e seus respectivos nomes e tipos

4. Na parte inferior da janela de propriedades do EULA, clique no botão **Revogar Contrato de Licença**.

Se existirem objetos (pacotes de instalação e suas respectivas tarefas) que impeçam a revogação do EULA, a notificação correspondente será exibida. 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.

5. 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).

Para renovar uma licença expirada ou uma licença 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 expiradas** ao lado de uma notificação.

A janela **LICENÇAS DA KASPERSKY** é aberta, permitindo visualiza e renovar licenças.

2. Clique no link **Renovar licença** ao lado da licença necessária.

Ao clicar no link de renovação da licença, você concorda em transferir à Kaspersky as seguintes informações sobre o Kaspersky Security Center: a versão, a localização de uso, a ID de licença do software (ou seja, a ID da licença sendo renovada), se a licença foi comprada via empresa parceira ou não.

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

A licença foi renovada.

No Kaspersky Security Center 14 Web 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

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 14 Linux redireciona seu acesso para a página da web relacionada no site da Kaspersky para saber mais sobre essa 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.

Configurar a 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 iniciar, assegure-se de que você tenha feito o seguinte:

- [Servidor de Administração do Kaspersky Security Center instalado com êxito](#)
- [Kaspersky Security Center 14 Web Console instalado](#)
- Cenário principal de instalação do Kaspersky Security Center concluído
- Concluiu o [Assistente de Início Rápido](#) ou criou manualmente as seguintes políticas e tarefas 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

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 Kaspersky instalados nos dispositivos gerenciados, você pode usar [duas abordagens de gerenciamento de segurança diferentes](#): centrado no dispositivo ou centrado no usuário. Essas duas abordagens também podem ser combinadas.

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: [Como configurar a tarefa de grupo para atualizar o Kaspersky Endpoint Security](#).

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.

[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 a 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 você quer controlar incidentes de segurança relacionados a 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

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.

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha [instalado o Servidor de Administração do Kaspersky Security Center](#) e o [Kaspersky Security Center 14 Web Console](#). Você pode também considerar o [gerenciamento de segurança centrado no usuário](#) como uma alternativa ou opção adicional à abordagem centrada no dispositivo. Saiba mais sobre [duas abordagens de gerenciamento](#).

Fases

O cenário de gerenciamento centrado no dispositivo dos aplicativos Kaspersky consiste nas seguintes etapas:

1 Configurar as 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 cria a política padrão do Kaspersky Endpoint Security for Linux. Se tiver concluído o processo de configuração usando este Assistente, você não precisará criar uma nova política para este aplicativo.

Se você tiver uma estrutura hierárquica de vários Servidores de Administração e/ou grupos de administração, os Servidores de Administração secundários e os grupos de administração secundários herdarão as políticas do Servidor de Administração principal por padrão. Você pode forçar a herança pelos grupos secundários e Servidores de Administração 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 ficarão disponíveis 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, tendo a configuração de hardware específica ou marcada com [tags](#) específicas. Use tags para filtrar dispositivos que atendem a critérios específicos. Por exemplo, você pode criar uma tag denominada *CentOS*, marcar todos os dispositivos executando o sistema operacional CentOS com essa tag e especificar essa tag como uma condição de ativação para um perfil da política. Como resultado, os aplicativos Kaspersky instalados em todos os dispositivos executando o CentOS serão gerenciados por seu próprio perfil da política.

Instruções de como proceder:

- o [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

Por padrão, o Kaspersky Security Center sincroniza automaticamente o Servidor de Administração com os dispositivos gerenciados a cada 15 minutos. 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 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.

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha [instalado com êxito o Servidor de Administração do Kaspersky Security Center](#) e o [Kaspersky Security Center 14 Web Console](#) e concluído o cenário de implementação principal. 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 as 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 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.

Se você tiver uma estrutura hierárquica de vários Servidores de Administração e/ou grupos de administração, os Servidores de Administração secundários e os grupos de administração secundários herdarão as políticas do Servidor de Administração principal por padrão. Você pode forçar a herança pelos grupos secundários e Servidores de Administração 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 ficarão disponíveis 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

Por padrão, o Kaspersky Security Center sincroniza automaticamente o Servidor de Administração com os dispositivos gerenciados a cada 15 minutos. 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 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 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 retardo aleatório automaticamente para início da tarefa** estiver marcada.

Configurações de política do Agente de Rede

Para configurar uma política do Agente de Rede:

1. No menu principal, vá para **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.

Geral

Nesta guia, 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:
 - [Política ativa](#) ⓘ

Se esta opção estiver selecionada, a política é habilitada.
Por padrão, esta opção está selecionada.

- [Política inativa](#) ⓘ

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 grupos de administração aninhados, 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

Nessa guia, é possível configurar o registro 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**

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). Após clicar no tipo de evento, é possível 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.

Por exemplo, na seção **Advertência**, é possível configurar o tipo de evento **Ocorreu um incidente**. Os eventos podem acontecer, por exemplo, quando o [espaço livre em disco de um ponto de distribuição](#) for inferior a 2 GB (pelo menos 4 GB são necessários para instalar aplicativos e baixar atualizações remotamente). Para configurar o evento **Ocorreu um incidente**, clique nele e especifique onde armazenar os eventos ocorridos e como notificá-los.

Caso o agente de rede tenha detectado um incidente, é possível gerenciá-lo usando as [configurações de um dispositivo gerenciado](#).

Configurações do aplicativo

Configurações

Na seção **Configurações**, você pode configurar a política do Agente de Rede:

- [Tamanho máximo da fila de eventos, em MB](#) 

Neste campo, você pode especificar o espaço máximo na unidade que uma fila de eventos pode ocupar. O valor predefinido é 2 megabytes (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 Linux). 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.

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.

- [Detalhes dos aplicativos instalados](#) 

Se esta opção estiver ativada, as informações sobre os aplicativos instalados nos dispositivos clientes serão enviadas ao Servidor de Administração.

Por padrão, esta opção está ativada.

- [Detalhes do registro de hardware](#) 

O Agente de Rede instalado em um dispositivo envia informações sobre o hardware do dispositivo para o Servidor de Administração. Você pode exibir os detalhes do hardware nas propriedades do dispositivo.

Rede

A seção **Rede** inclui três subseções:

- **Conectividade**

- **Perfis de conexão**
- **Agendador de conexão**

Na subseção **Conectividade**, 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 **Conectar-se ao Servidor de Administração**, você poderá configurar a conexão ao Servidor de Administração e especificar o intervalo de tempo para a sincronização entre os dispositivos cliente e o Servidor de Administração:

- **[Intervalo de sincronização \(min.\)](#)** ⓘ

O Agente de Rede sincroniza o dispositivo gerenciado com o Servidor de Administração. Recomendamos definir o intervalo de sincronização (também conhecido como heartbeat) para 15 minutos a cada 10.000 dispositivos gerenciados.

Se o intervalo de sincronização estiver definido para menos de 15 minutos, a sincronização será realizada a cada 15 minutos. Se o intervalo de sincronização estiver definido como 15 minutos ou mais, a sincronização será realizada no intervalo de sincronização especificado.

- **[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 conseqüente carga inferior sobre o Servidor de Administração.

A carga na CPU do computador cliente pode aumentar.

Por padrão, esta caixa de seleção é marcada.

- **[Usar conexão SSL](#)** ⓘ

Se esta opção estiver ativada, a conexão com o Servidor de Administração é estabelecida através de uma porta segura via SSL.

Por padrão, esta opção está ativada.

- **[Use o gateway de conexão no 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.

Na subseção **Perfis de conexão** em **Rede**, você pode especificar as configurações do local da rede e ativar o modo ausente do escritório quando o Servidor de Administração não estiver disponível. As configurações na seção **Perfis de conexão** estão disponíveis somente em dispositivos que executam o Windows:

- [Configurações do local de rede](#)

As configurações da localização da rede definem as características da rede à qual o dispositivo cliente está conectado e especifica as regras para o Agente de Rede alternando de um perfil de conexão do Servidor de Administração a outro quando aquelas características da rede forem alteradas.

- [Perfis de conexão do Servidor de Administração](#)

Os perfis de conexão tem suporte somente para dispositivos que executam o Windows. Não recomendamos usar essa opção.

É possível visualizar e adicionar perfis à conexão do Agente de Rede com o Servidor de Administração. Nesta seção, você também pode criar regras para alternar o Agente de Rede para diferentes Servidores de Administração quando os seguintes eventos ocorrerem:

- Quando o dispositivo cliente se conectar a outra rede local
- Quando um dispositivo perde a conexão com a rede local da organização
- Quando o endereço do gateway de conexão for alterado ou o endereço do servidor DNS for modificado.

No grupo de configurações **Perfis de conexão**, nenhum novo item pode ser adicionado à lista **Perfis de conexão do Servidor de Administração**. Por isso, o botão **Adicionar** fica inativo. Os perfis de conexão predefinidos também não podem ser modificados.

- [Ativar modo ausente quando o Servidor de Administração não estiver disponível](#)

Se esta opção estiver marcada, no caso da conexão com este perfil, os aplicativos instalados no dispositivo cliente irão usar as políticas do modo ausente, assim como as políticas de ausência de escritório. Se a política de ausência do escritório não estiver definida para o aplicativo, a política ativa será usada.

Se esta opção estiver desativada, os aplicativos usarão as políticas ativas.

Por padrão, esta opção está desativada.

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. Você pode usar as seguintes opções para ativar a sondagem e definir a frequência:

- [Zeroconf](#) 

Se esta opção for ativada, o ponto de distribuição sondará automaticamente a rede com dispositivos IPv6 usando a [rede zero configuração](#) (também referida como *Zeroconf*). Nesse caso, a sondagem de intervalo de IP ativada é ignorada, porque o ponto de distribuição sonda toda a rede.

Para começar a usar o Zeroconf, as seguintes condições devem ser atendidas:

- O ponto de distribuição deve executar Linux.
- Você deve instalar o utilitário avahi-browse no ponto de distribuição.

Se essa opção estiver desativada, o ponto de distribuição não faz a sondagem com dispositivos IPv6y.

Por padrão, esta opção está desativada.

- [Intervalos de IPs](#) 

Se a opção estiver ativada, o Servidor de Administração automaticamente efetua a sondagem de conjuntos de IPs de acordo com o agendamento configurado ao clicar no link **Definir agendamento da sondagem**.

Se esta opção estiver ativada, o Servidor de Administração não faz a sondagem dos intervalos de IP.

A frequência de sondagem de conjuntos de IPs para versões do Agente de Rede anteriores a 10.2 pode ser configurada no campo **Intervalo de sondagem (min.)**. O campo está disponível se a opção estiver 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 a caixa de seleção estiver ativada, você pode especificar as credenciais para a autenticação do servidor proxy.

Por padrão, esta caixa de seleção está desmarcada.

- Nome do usuário

- Senha

Atualizações (pontos de distribuição)

Na seção **Atualizações (pontos de distribuição)**, é possível ativar o [recurso de download de arquivos diff](#), para que os pontos de distribuição recebam atualizações na forma de arquivos diff dos servidores de atualização da Kaspersky.

Histórico de revisões

Nessa guia, é possível visualizar a lista de revisões de política e [reverter alterações](#) feitas na política, se necessário.

Alterando a prioridade para as regras de migração de dispositivos

Todas as regras para migrar dispositivo têm prioridades.

Para aumentar ou diminuir a prioridade de uma regra móvel:

mov a regra para cima ou para baixo na lista, respectivamente, usando o mouse.

Tarefas

Esta seção descreve as tarefas utilizadas pelo Kaspersky Security Center.

Sobre as tarefas

O Kaspersky Security Center gerencia os aplicativos de segurança da 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 de um aplicativo específico podem ser criadas usando o Kaspersky Security Center 14 Web Console apenas se o plugin de gerenciamento desse aplicativo estiver instalado no Kaspersky Security Center 14 Web Console Server.

As tarefas podem ser realizadas no Servidor de Administração e em dispositivos.

As tarefas executadas no Servidor de Administração incluem o seguinte:

- Distribuição automática de relatórios
- Download de atualizações para o repositório
- Backup de dados do Servidor de Administração
- Manutenção do banco de dados

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 por meio do uso do Kaspersky Security Center 14 Web Console ou pelo usuário de um dispositivo remoto (por exemplo, por meio 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. Uma tarefa de grupo também afeta (opcionalmente) os dispositivos que foram conectados aos Servidores de Administração secundários e virtuais implementados no grupo ou em algum dos seus subgrupos.

- *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 qualquer número de 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 no log de eventos do sistema operacional em cada dispositivo, no log de eventos do sistema operacional: do Servidor de Administração 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) 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

Para criar uma tarefa:

1. No menu principal, vá para **DISPOSITIVOS** → **TAREFAS**.
2. Clique em **Adicionar**.
O Assistente para Adicionar Tarefas é iniciado. 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.

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 a tarefa manualmente a qualquer momento.

Para iniciar uma tarefa manualmente:

1. No menu principal, vá para **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**.

Visualizando a lista de tarefas

Você pode ver a lista de tarefas criadas no Kaspersky Security Center Linux.

Para visualizar a lista de tarefas,

Acesse **DISPOSITIVOS** → **TAREFAS**.

A lista de tarefas é exibida. As tarefas são agrupadas pelos nomes dos aplicativos aos quais estão relacionados. Por exemplo, a tarefa *Instalar o aplicativo remotamente* está relacionada ao Servidor de Administração e a tarefa *Atualizar*, ao Kaspersky Endpoint Security for Linux.

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**.

Configurações de tarefa gerais

Esta seção lista as configurações que podem ser visualizadas e especificadas para tarefas.

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.

- 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).

- **[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 de agendamento de tarefas:

- **[Início agendado](#)**

Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

- **[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.

- **[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.

- **[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 Linux.

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.

- **[Manualmente](#)**

A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

Por padrão, esta opção está ativada.

- **[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 e a hora de início é 18h.

- [Quando novas atualizações são baixadas no repositório](#)

A tarefa é executada após as atualizações serem baixadas no repositório. Por exemplo, pode ser necessário usar esse agendamento para a tarefa *Atualizar*.

- [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.

- [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 retardo 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 retardo 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.

- Dispositivos aos quais a tarefa será atribuída:

- [Selecionar os dispositivos na rede detectados pelo Servidor de Administração](#)

A tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.

Por exemplo, pode ser necessário usar esta opção em uma tarefa de instalação do Agente de Rede em dispositivos não atribuídos.

- [Especificar os endereços do dispositivo manualmente ou importar os endereços da lista](#) 

Você pode especificar 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.

- [Atribuir uma 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.

- 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 uma 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.

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 da [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 avançado:

- [Ativar dispositivo antes que a tarefa seja iniciada pelo Wake-On-LAN \(min.\)](#) ⓘ

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 o dispositivo depois de concluir a tarefa**. Esta opção pode ser encontrada na mesma janela.

Por padrão, esta opção está desativada.

- [Desligar dispositivo depois que a tarefa for concluída](#) ⓘ

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 tarefa se estiver em execução há mais de (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.

- Configurações de notificação:

- Bloco **Armazenar histórico de tarefas:**

- **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 Syslog de cada dispositivo cliente.

Por padrão, esta opção está desativada.

- **Armazenar no log de eventos do SO no Servidor de Administração** 

Os eventos de aplicativo relacionados à execução da tarefa em todos os dispositivos cliente do escopo da tarefa são armazenados centralmente no Log de Eventos do Syslog do sistema operacional (SO) do Servidor de Administração.

Por padrão, esta opção está desativada.

- **Salvar todos os eventos** 

Se esta opção estiver selecionada, todos os eventos relacionados à tarefa serão salvos nos logs de eventos.

- **Salvar eventos relacionados ao progresso da tarefa** 

Se esta opção estiver selecionada, apenas os eventos relacionados à execução da tarefa serão salvos nos logs de eventos.

- [Salvar apenas os resultados da execução da tarefa](#) ?

Se esta opção estiver selecionada, apenas os eventos relacionados aos resultados da tarefa serão salvos nos logs de eventos.

- [Notificar administrador sobre os resultados de execução de tarefa](#) ?

Você pode selecionar os métodos pelos quais os administradores recebem notificações sobre os resultados de execução da tarefa: por e-mail, por SMS e pela execução de um arquivo executável. Para configurar a notificação, clique em link **Configurações**.

Por padrão, todos os métodos de notificação estão desativados.

- [Notificar somente erros](#) ?

Se esta opção estiver ativada, os administradores serão notificados apenas quando uma execução de tarefa for concluída com um erro.

Se esta opção estiver desativada, os administradores serão notificados após cada conclusão de execução de tarefa.

Por padrão, esta opção está ativada.

- Configurações de segurança.

- Configurações do escopo da tarefa.

Dependendo de como o escopo da tarefa é determinado, as seguintes configurações estão presentes:

- [Dispositivos](#) ?

Se o escopo de uma tarefa for determinado por um grupo de administração, você pode exibir e visualizar esse grupo. Nenhuma alteração está disponível nesse ponto. No entanto, você pode definir **Exclusões do escopo da tarefa**.

Se o escopo de uma tarefa for determinado por uma lista de dispositivos, você pode alterar essa lista adicionando e removendo dispositivos.

- [Seleção de dispositivos](#) ?

Você pode alterar a seleção de dispositivos aos quais a tarefa é aplicada.

- [Exclusões do escopo da tarefa](#) ?

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 da revisão.

Iniciar o assistente para alterar a senha das tarefas

Para uma tarefa não local, você pode especificar uma conta na qual a tarefa deve ser executada. Você pode especificar a conta durante a criação da tarefa ou nas propriedades de uma tarefa existente. Se a conta especificada for usada de acordo com as instruções de segurança da organização, essas instruções poderão exigir a alteração periódica da senha da conta. Quando a senha da conta expirar e você definir uma nova, as tarefas não serão iniciadas até que você especifique a nova senha válida nas propriedades da tarefa.

O Assistente para Alterar a Senha das Tarefas permite substituir automaticamente a senha antiga pela nova em todas as tarefas em que a conta esteja especificada. Como alternativa, você pode alterar esta senha manualmente nas propriedades de cada tarefa.

Para iniciar o Assistente para Alterar a Senha das Tarefas:

1. Na guia **DISPOSITIVOS**, selecione **TAREFAS**.
2. Clique em **Gerenciar as credenciais de contas para iniciar tarefas**.

Siga as instruções do Assistente.

Etapa 1. Especificar as credenciais

Especifique novas credenciais atualmente válidas em seu sistema. Quando você passa para a próxima etapa do Assistente, o Kaspersky Security Center verifica se o nome da conta especificado corresponde ao nome da conta nas propriedades de cada tarefa não local. Se os nomes das contas corresponderem, a senha nas propriedades da tarefa será automaticamente substituída pela nova.

Para especificar a nova conta, selecione uma opção:

- [Usar a conta atual](#) 

O Assistente usa o nome da conta na qual você está conectado atualmente ao Kaspersky Security Center 14 Web Console. Em seguida, especifique manualmente a senha da conta no campo **Senha atual para usar em tarefas**.

- [Especificar uma conta diferente](#) 

Especifique o nome da conta na qual as tarefas devem ser iniciadas. Em seguida, especifique a senha da conta no campo **Senha atual para usar em tarefas**.

Se você preencher o campo **Senha anterior (opcional; caso você deseje substituí-la pela atual)**, o Kaspersky Security Center substitui a senha apenas para as tarefas nas quais o nome da conta e a senha antiga são encontrados. A substituição é realizada automaticamente. Em todos os outros casos, você precisa escolher uma ação a ser executada na próxima etapa do Assistente.

Etapa 2. Selecionar uma ação a ser executada

Se você não especificou a senha antiga na primeira etapa do Assistente ou a senha antiga especificada não correspondeu às senhas nas propriedades da tarefa, deverá escolher uma ação a ser executada para as tarefas encontradas.

Para escolher uma ação para uma tarefa:

1. Marque a caixa de seleção ao lado da tarefa para a qual deseja escolher uma ação.
2. Execute um dos seguintes procedimentos:
 - Para remover a senha nas propriedades da tarefa, clique em **Excluir as credenciais**.
A tarefa é alternada para ser executada na conta padrão.
 - Para substituir a senha por uma nova, clique em **Impor alteração da senha mesmo se a senha antiga esteja incorreta ou não foi fornecida**.
 - Para cancelar a alteração da senha, clique em **Nenhuma ação está selecionada**.

As ações escolhidas são aplicadas depois que você passar para a próxima etapa do Assistente.

Etapa 3. Visualizar os resultados

Na última etapa do assistente, visualize os resultados para cada uma das tarefas encontradas. Para concluir o Assistente, pressione o botão **Concluir**.

Visualização de resultados da execução de tarefas armazenados no Servidor de Administração

O Kaspersky Security Center Linux permite visualizar resultados de execução para tarefas de grupo, tarefas para dispositivos específicos e tarefas do Servidor de Administração. Não podem ser visualizados resultados de execução para tarefas locais.

Para visualizar os resultados da tarefa:

1. Na janela de propriedades da tarefa, selecione a seção **Geral**.
2. Clique no link **Resultados** para abrir a janela **Resultados da tarefa**.

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. Selecione **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.

Geral

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.

- **Grupo** 

Grupo de administração que inclui o dispositivo cliente.

- **Última atualização** 

Data em que os bancos de dados ou os aplicativos foram atualizados por último no dispositivo.

- **Última visualização** 

Data e hora de quando o dispositivo esteve por último visível na rede.

- **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.

- **Não desconectar do Servidor de Administração** 

Caso esta opção seja ativada, será mantida uma conectividade contínua entre o dispositivo gerenciado e o Servidor de Administração. Convém utilizar essa opção caso os servidores push, que fornecem essa 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.

Rede

A seção **Rede** fornece as seguintes informações sobre as propriedades da rede do dispositivo cliente:

- [Endereço IP](#) ⓘ

Endereço IP do dispositivo.

- [Domínio do Windows](#) ⓘ

Grupo de trabalho que contém o dispositivo.

- [Nome DNS](#) ⓘ

Nome do domínio DNS do dispositivo cliente.

- [Nome do NetBIOS](#) ⓘ

Nome do dispositivo cliente.

Sistema

A seção **Sistema** fornece informações sobre o sistema operacional instalado no dispositivo cliente.

Proteção

A seção **Proteção** fornece informações sobre o status atual da proteção antivírus no 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.

- [Todos os problemas](#) 

Esta tabela contém uma lista completa de problemas detectados pelos aplicativos gerenciados instalados no dispositivo cliente. Cada problema é acompanhado por um status, que o aplicativo sugere que você atribua ao dispositivo para esse problema.

- [Proteção em tempo real](#) 

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 sob demanda](#) 

Data e hora em que a verificação de vírus foi executada por último no dispositivo cliente.

- [Número total de ameaças detectadas](#) 

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.

- [Ameaças ativas](#) 

Número de arquivos não processados no dispositivo cliente.

Este campo ignora o número de arquivos não processados nos dispositivos móveis.

Status do dispositivo definido pelo aplicativo

A seção **Status do dispositivo definido pelo aplicativo** fornece informações sobre o status do dispositivo definido pelo aplicativo gerenciado instalado no dispositivo. O status do dispositivo pode ser diferente do definido pelo Kaspersky Security Center Linux.

Aplicativos

A seção **Aplicativos** 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 ativas e perfis da política

A seção **Políticas ativas e perfis de políticas** lista as políticas e perfis de políticas atualmente ativos no dispositivo gerenciado.

Tarefas

Na seção **Tarefas**, você pode gerenciar tarefas de dispositivo cliente: exibir a lista de tarefas existentes, criar novas, remover, iniciar e parar tarefas, modificar as suas configurações e exibir 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 seção **Eventos** exibe os eventos registrados no Servidor de Administração para o dispositivo cliente selecionado.

Tags

Na seção **Tags**, você poderá gerenciar a lista de palavras-chave que são usadas para localizar dispositivos cliente: exibir a lista de tags existentes, atribuir tags da lista, configurar regras de identificação automática, adicionar novas tags e renomear os antigos e excluir tags.

Arquivos executáveis

A seção **Arquivos executáveis** 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](#) 

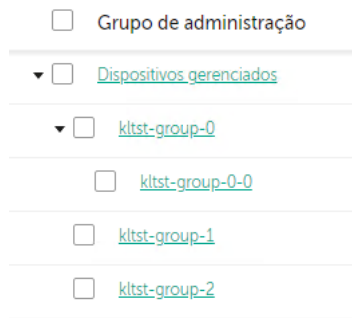
Clique no botão **Propriedades** para exibir e configurar o ponto de distribuição com o qual o dispositivo interage.

Registro de hardware

Na seção **Registro de hardware**, você poderá visualizar as informações sobre o hardware instalado no dispositivo cliente.

Criação de grupos de administração

Imediatamente após a instalação do Kaspersky Security Center, a hierarquia dos grupos de administração contém apenas um grupo de administração chamado **Dispositivos gerenciados**. Ao criar uma hierarquia de grupos de administração, você poderá adicionar dispositivos e máquinas virtuais à pasta **Dispositivos gerenciados**, e adicionar grupos aninhados (veja a figura abaixo).



Exibir hierarquia de grupos de administração

Para criar um grupo de administração:

1. Acesse **DISPOSITIVOS** → **HIERARQUIA DE GRUPOS**.
2. Na estrutura do grupo de administração, selecione o grupo de administração que deve incluir o novo grupo de administração.
3. Clique no botão **Adicionar**.
4. Na janela **Nome do novo grupo de administração** que se abre, insira um nome para o grupo e clique no botão **Adicionar**.

Um novo grupo de administração com o nome especificado aparece na hierarquia dos grupos de administração.

Para criar a estrutura de grupos de administração:

1. Acesse **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.

Regras de migração de dispositivos

Recomendamos definir a alocação automática de dispositivos em grupos de administração através das *regras de migração de dispositivos*. Uma regra para migrar dispositivo compõe-se de três partes principais: um nome, uma [condição de execução](#) (expressão lógica com os atributos de dispositivo) e um grupo de administração alvo. Uma regra move um dispositivo para o grupo de administração alvo se os atributos do dispositivo atendam a condição de execução da regra.

Todas as regras para migrar dispositivo têm prioridades. O Servidor de Administração verifica os atributos do dispositivo quanto a se eles atendem a condição de execução de cada regra, na ordem ascendente da prioridade. Se os atributos do dispositivo atenderem a condição de execução de uma regra, o dispositivo é movido para o grupo alvo, portanto o processamento de regra é completo para este dispositivo. 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).

As regras para migrar dispositivo podem ser criadas implicitamente. Por exemplo, nas propriedades de um pacote de instalação ou de uma tarefa de instalação remota, você pode especificar o grupo de administração para o qual o dispositivo deve ser movido após que Agente de Rede seja instalado nele. Além disso, as regras para migrar dispositivos podem ser criadas explicitamente pelo administrador do Kaspersky Security Center Linux na seção **DISPOSITIVOS** → **REGRAS DE MIGRAÇÃO**.

Por padrão, uma regra para mover dispositivo é destinada para a alocação inicial de uma só vez de dispositivos aos grupos de administração. A regra move os dispositivos do grupo dispositivos não atribuídos somente uma vez. Se um dispositivo foi movido uma vez por esta regra, a regra nunca mais o moverá novamente, mesmo se você devolver o dispositivo ao grupo dispositivos não atribuídos manualmente. Esta é a forma recomendada de aplicar regras para mover.

Você pode migrar dispositivos que já foram alocados à alguns dos grupos de administração. Para fazer isso, nas propriedades de uma regra, desmarque a caixa de seleção **Somente mover os dispositivos que não pertencem a um grupo de administração**.

Aplicar regras para mover aos dispositivos que já foram alocados à alguns dos grupos de administração, aumenta significativamente a carga do Servidor de Administração.

Você pode criar uma regra para mover que iria afetar um único dispositivo repetidamente.

Nós recomendamos com ênfase que você evite mover um dispositivo único de um grupo para outro repetidamente (por exemplo, para poder aplicar uma política especial àquele dispositivo, executar uma tarefa de grupo especial, ou atualizar o dispositivos através de um ponto de distribuição específico).

Tais cenários não são compatíveis, porque eles aumentam a carga no Servidor de Administração e o tráfego da rede para um grau extremo. Estes cenários também estão em conflito com os princípios operacionais do Kaspersky Security Center Linux (em particular na área de direitos de acesso, eventos e relatórios). Outra solução deve ser encontrada, por exemplo, por meio do uso de perfis da política, tarefas para [seleções de dispositivos](#), atribuição de [Agentes de Rede de acordo com o cenário padrão](#), e assim por diante.

Criar regras para mover dispositivos

É possível configurar as regras de migração de dispositivos, ou seja, as regras que alocam automaticamente os dispositivos nos grupos de administração.

Para criar uma regra para mover dispositivos:

1. No menu principal, acesse a guia **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.

- **[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, então a cada nova instalação 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.

- Regra aplicada continuamente.

A regra é aplicada de acordo com o agendamento que o Servidor de Administração configura automaticamente (normalmente a cada várias horas).

- [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.

- [Ativar regra](#) 

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.

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 maior a posição na lista, maior a prioridade da regra. 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. No menu principal, acesse a guia **DISPOSITIVOS** → **REGRAS DE MIGRAÇÃO**.

Também é possível selecionar **DESCOBERTA E IMPLEMENTAÇÃO** → **IMPLEMENTAÇÃO E ATRIBUIÇÃO** e, no menu, selecionar **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.

- [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, então a cada nova instalação 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.

- Regra aplicada continuamente.

A regra é aplicada de acordo com o agendamento que o Servidor de Administração configura automaticamente (normalmente a cada várias horas).

- [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.

- [Ativar regra](#) ?

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.

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.

Condições para migrar uma regra de um dispositivo

Ao [criar](#) ou [copiar](#) uma regra para migrar dispositivos cliente para grupos de administração, na guia **Condições da regra**, as condições para [migrar os dispositivos](#) serão definidas. Para determinar quais dispositivos migrar, será necessário usar os seguintes critérios:

- Tags atribuídas a dispositivos clientes.
- Parâmetros de rede. Por exemplo, é possível migrar os dispositivos com os endereços IP a partir de um intervalo especificado.
- Aplicativos gerenciados e instalados em dispositivos clientes, por exemplo, o Agente de Rede ou o Servidor de Administração.
- Máquinas virtuais, que são os dispositivos clientes.

Abaixo, é possível encontrar a descrição sobre a especificação dessas informações em uma regra de movimentação de dispositivos.

Caso especifique várias condições na regra, o operador lógico AND funcionará e todas as condições serão aplicadas ao mesmo tempo. Caso não selecione nenhuma opção ou alguns campos sejam deixados em branco, essas condições não serão aplicadas.

Guia Tags

Nesta guia, é possível configurar uma regra de migração de dispositivo de acordo com as [tags de dispositivo](#) adicionadas anteriormente nas descrições dos dispositivos clientes. Para fazer isso, selecione as tags necessárias. Além disso, é possível ativar as seguintes opções:

- [Aplicar aos dispositivos sem tags especificadas](#) 

Caso esta opção esteja habilitada, todos os dispositivos com as tags especificadas serão excluídos de uma regra de migração de dispositivos. Caso esta opção esteja desabilitada, a regra de migração de dispositivo será aplicável aos dispositivos com todas as tags selecionadas.

Por padrão, esta opção está desativada.

- [Aplicar se pelo menos uma tag especificada corresponder](#) 

Caso esta opção esteja habilitada, uma regra de migração de dispositivo será aplicável aos dispositivos clientes com pelo menos uma das tags selecionadas. Caso esta opção esteja desabilitada, a regra de migração de dispositivo será aplicável aos dispositivos com todas as tags selecionadas.

Por padrão, esta opção está desativada.

Guia Rede

Nesta guia, é possível especificar os dados de rede dos dispositivos que uma regra de migração de dispositivo considera:

- [Nome de DNS do dispositivo](#) ?

Nome do domínio DNS do dispositivo cliente que deseja migrar. Preencha este campo se sua rede incluir um servidor DNS.

- [Domínio DNS](#) ?

Uma regra de migração de dispositivo será aplicável a todos os dispositivos incluídos no sufixo DNS principal especificado. Preencha este campo se sua rede incluir um servidor DNS.

- [Intervalo IP](#) ?

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.

- [Endereço IP para conexão com o Servidor de Administração](#) ?

Caso esta opção esteja habilitada, será possível definir os endereços IP pelos quais os dispositivos clientes serão conectados ao Servidor de Administração. Para fazer isso, especifique o intervalo de IP que inclui todos os endereços IP necessários.

Por padrão, esta opção está desativada.

- [Perfil de conexão alterado](#) ?

Selecione um dos seguintes valores:

- **Sim.** Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente com um perfil de conexão alterado.
- **Não.** A regra de migração de dispositivo será aplicável apenas aos dispositivos cliente cujo perfil de conexão não foi alterado.
- **Nenhum valor está selecionado.** A condição não se aplica.

- [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 migração de dispositivo será aplicável apenas aos dispositivos cliente gerenciados pelo Servidor de Administração atual.
- **Nenhum valor está selecionado.** A condição não se aplica.

Nesta guia, é possível configurar uma regra de migração de dispositivo de acordo com os aplicativos gerenciados e sistemas operacionais instalados nos dispositivos cliente:

- [Agente de Rede instalado](#)

Selecione um dos seguintes valores:

- **Sim.** Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente com o Agente de Rede instalado.
- **Não.** A regra de migração de dispositivo será aplicável apenas aos dispositivos cliente nos quais o Agente de Rede não está instalado.
- **Nenhum valor está selecionado.** A condição não se aplica.

- [Aplicativos](#)

Especifique quais aplicativos gerenciados devem ser instalados em dispositivos cliente para que uma regra de migração de dispositivo seja aplicável a esses dispositivos. Por exemplo, é possível selecionar **Agente de Rede do Kaspersky Security Center 14** ou **Servidor de Administração do Kaspersky Security Center 14**.

Caso nenhum aplicativo gerenciado seja selecionado, a condição não será aplicável.

- [Versão do sistema operacional](#)

É possível selecionar os dispositivos cliente de acordo com a versão do sistema operacional. Para isso, especifique os sistemas operacionais que devem ser instalados nos dispositivos cliente. Assim, uma regra de migração de dispositivo será aplicável aos dispositivos cliente com os sistemas operacionais selecionados.

Caso esta opção não seja habilitada, a condição não será aplicável. Por padrão, a opção está desativada.

- [Tipo de bit do sistema operacional](#)

É possível selecionar os dispositivos cliente pelos tamanhos de bits do sistema operacional. No campo **Tipo de bit do sistema operacional**, será possível selecionar um dos seguintes valores:

- Desconhecido
- x86
- AMD64
- IA64

Para verificar o tamanho de bits do sistema operacional dos dispositivos cliente:

1. No menu principal, acesse a seção **DISPOSITIVOS** → **DISPOSITIVOS GERENCIADOS**.
2. Clique no botão **Configurações de colunas** (☰) à direita.
3. Selecione a opção **Tipo de bit do sistema operacional** e clique no botão **Salvar**.

Depois disso, o tamanho do bit do sistema operacional será exibido para cada dispositivo gerenciado.

- [Versão do service pack do sistema operacional](#)

Nesse campo, você poderá 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.

- [Certificado do usuário](#) ⓘ

Selecione um dos seguintes valores:

- **Instalado.** Uma regra de migração de dispositivo será aplicável apenas aos dispositivos móveis com um certificado móvel.
- **Não instalado.** A regra de migração de dispositivo se aplicável apenas aos dispositivos móveis sem um certificado móvel.
- **Nenhum valor está selecionado.** A condição não se aplica.

- [Compilação do sistema operacional](#) ⓘ

Esta configuração é aplicável somente aos sistemas operacionais Windows.

Você pode especificar se o sistema operacional selecionado deve ter um número de compilação igual, anterior ou posterior. Também é possível configurar a regra de migração de dispositivo para todos os números de compilação, exceto o especificado.

- [Número da versão do sistema operacional](#) ⓘ

Esta configuração é aplicável somente aos sistemas operacionais Windows.

É possível especificar se o sistema operacional selecionado ter um número de versão igual, anterior ou posterior. Também é possível configurar uma regras de migração de dispositivo para todos os números de versão, exceto o especificado.

Guia Máquinas virtuais

Na guia, é possível configurar a migração de dispositivo de acordo com o fato de que os dispositivos cliente sejam máquinas virtuais ou parte da Virtual Desktop Infrastructure (VDI):

- [Esta é uma máquina virtual](#) ⓘ

Na lista suspensa, é possível selecionar os seguintes itens:

- **N/A.** A condição não se aplica.
- **Não.** Migrar dispositivos que não sejam máquinas virtuais.
- **Sim.** Migrar dispositivos que sejam máquinas virtuais.

- **Tipo de máquina virtual**
- **[Parte da Virtual Desktop Infrastructure](#)** 

Na lista suspensa, é possível seleccionar os seguintes itens:

- **N/A.** A condição não se aplica.
- **Não.** Migre os dispositivos que não fazem parte da VDI.
- **Sim.** Migre os dispositivos que fazem parte da VDI.

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 seleccionado. Esta seção descreve como adicionar dispositivos a um grupo de administração manualmente.

Para adicionar manualmente um ou mais dispositivos a um grupo de administração seleccionado:

1. Acesse **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 um nome DNS do 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 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.

Para migrar um ou diversos dispositivos 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, vá para **DISPOSITIVOS** → **Grupos <group name> DISPOSITIVOS GERENCIADOS**.
 - Para abrir o grupo **DISPOSITIVOS NÃO ATRIBUÍDOS**, vá para **DESCOBERTA E IMPLEMENTAÇÃO** → **DISPOSITIVOS NÃO ATRIBUÍDOS**.
2. Marque a caixa de seleção ao lado dos dispositivos que deseja migrar para um grupo diferente.
3. Clique no botão **Migrar para grupo**.
4. Na hierarquia de grupos de administração, marque a caixa de seleção ao lado do grupo de administração para o qual deseja migrar os dispositivos selecionados.
5. Clique no botão **Migrar**.

Os dispositivos selecionados são movidos para o grupo de administração selecionado.

Alterar o Servidor de Administração para dispositivos cliente

Você pode alterar o Servidor de Administração para dispositivos clientes específicos. Para isso, use a tarefa *Alterar o Servidor de Administração*.

Para alterar o Servidor de Administração que gerencia dispositivos cliente para outro servidor:

1. Conecte-se ao Servidor de Administração que gerencia os dispositivos.

2. [Crie](#) a tarefa do Servidor de Administração.

O Assistente para Adicionar Tarefas é iniciado. Siga as instruções do Assistente. Na janela **Nova tarefa** do Assistente para Adicionar Tarefa, selecione o aplicativo **Kaspersky Security Center 14** e o tipo de tarefa **Alterar o Servidor de Administração**. Depois disso, especifique os dispositivos para os quais você deseja alterar o Servidor de Administração:

- [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 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.

3. 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.

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 **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 Linux 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 Linux leva em consideração o sinalizador de visibilidade do dispositivo na rede (consulte a tabela abaixo). Se o Kaspersky Security Center Linux 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Parado. Pausada. Executando.
A verificação de vírus não é executada há muito tempo	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas a tarefa de verificação de vírus não foi executada 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.	<ul style="list-style-type: none"> O botão de alternar é desativado. O botão de alternar é ativado.

A licença expirou	O dispositivo está visível na rede, mas a licença expirou.	<ul style="list-style-type: none"> • 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.
Incidentes não processados detectados	Alguns incidentes não processados foram encontrados no dispositivo. Os incidentes podem ser criados automaticamente, através de aplicativos da Kaspersky gerenciados instalados no dispositivo cliente, ou manualmente pelo administrador.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 <i>Crítico</i> ou <i>Advertência</i> é alterado para o status <i>OK</i> 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.	<ul style="list-style-type: none"> • 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.	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.	<ul style="list-style-type: none"> • O botão de alternar é desativado. • O botão de alternar é ativado.

O Kaspersky Security Center Linux permite definir a troca 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*.

Se você atualizar o Kaspersky Security Center Linux da versão anterior, os valores da condição **Os bancos de dados estão desatualizados** para atribuir o status *Crítico* ou *Aviso* não mudam.

Quando o Kaspersky Security Center Linux 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. Abra a janela Propriedades em uma das seguintes formas:
 - Na pasta **Políticas** no menu de contexto de uma política de Servidor de Administração, selecione **Propriedades**.
 - Selecione **Propriedades** no menu de contexto de um grupo de administração.
2. Na janela de propriedades que se abre, no painel **Seções**, selecione **Status do dispositivo**.
3. No painel direito, na seção **Se especificados, definir como Crítico**, selecione a caixa de seleção ao lado de uma condição na lista.

No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

4. Defina o valor necessário para a condição selecionada.
Você pode definir valores para algumas condições, mas não para todas.
5. 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. Abra a janela Propriedades em uma das seguintes formas:

- Na pasta **Políticas**, no menu de contexto da política de Servidor de Administração, selecione **Propriedades**.
 - Selecione **Propriedades** no menu de contexto do grupo de administração.
2. Na janela de propriedades que se abre, no painel **Seções**, selecione **Status do dispositivo**.
 3. No painel direito, na seção **Se especificados, definir como Advertência**, selecione a caixa de seleção ao lado de uma condição na lista.

No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

4. Defina o valor necessário para a condição selecionada.
Você pode definir valores para algumas condições, mas não para todas.
5. Clique em **OK**.

Quando as condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Advertência*.

Políticas e perfis da política

No Kaspersky Security Center 14 Web Console, você pode criar políticas para aplicativos Kaspersky. Esta seção descreve políticas e perfis da política e fornece instruções para criá-las e modificá-las.

Sobre as políticas e perfis de política

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 fornece uma única política para cada aplicativo Kaspersky em um grupo de administração. Uma política possui um dos seguintes status:

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.
Inativa	Uma política que não é aplicada atualmente a um dispositivo.
Remota	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.
- 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.

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
	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 <i>desbloqueado</i> .
	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 <i>bloqueado</i> .

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:

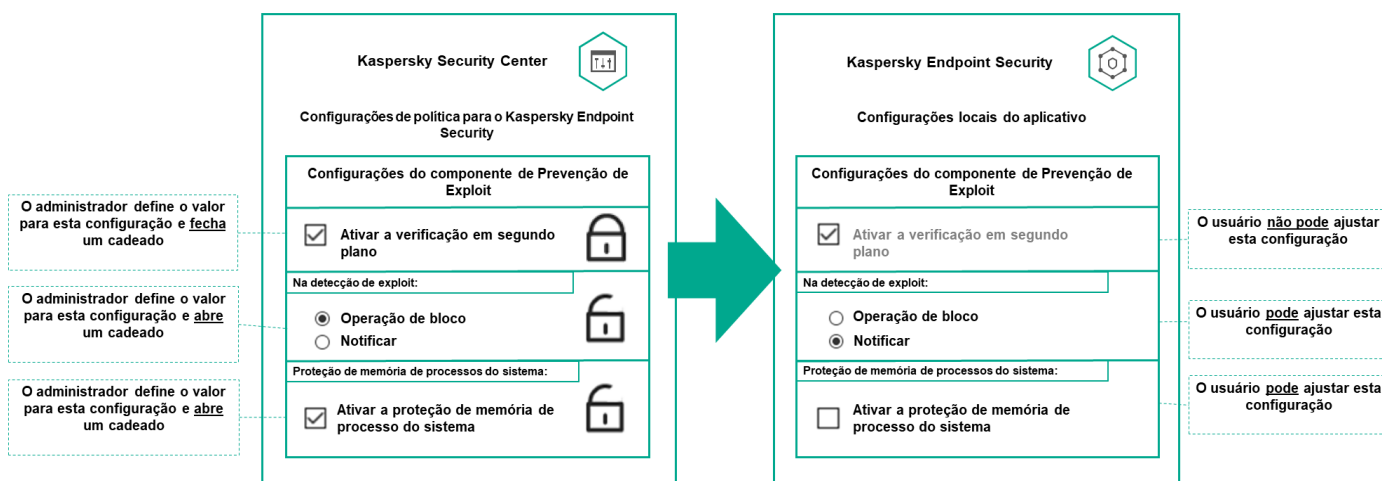
- Configurações de bloqueio para uma política de subgrupo de administração
- Bloqueando as configurações de um aplicativo da Kaspersky em um dispositivo gerenciado

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 local 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

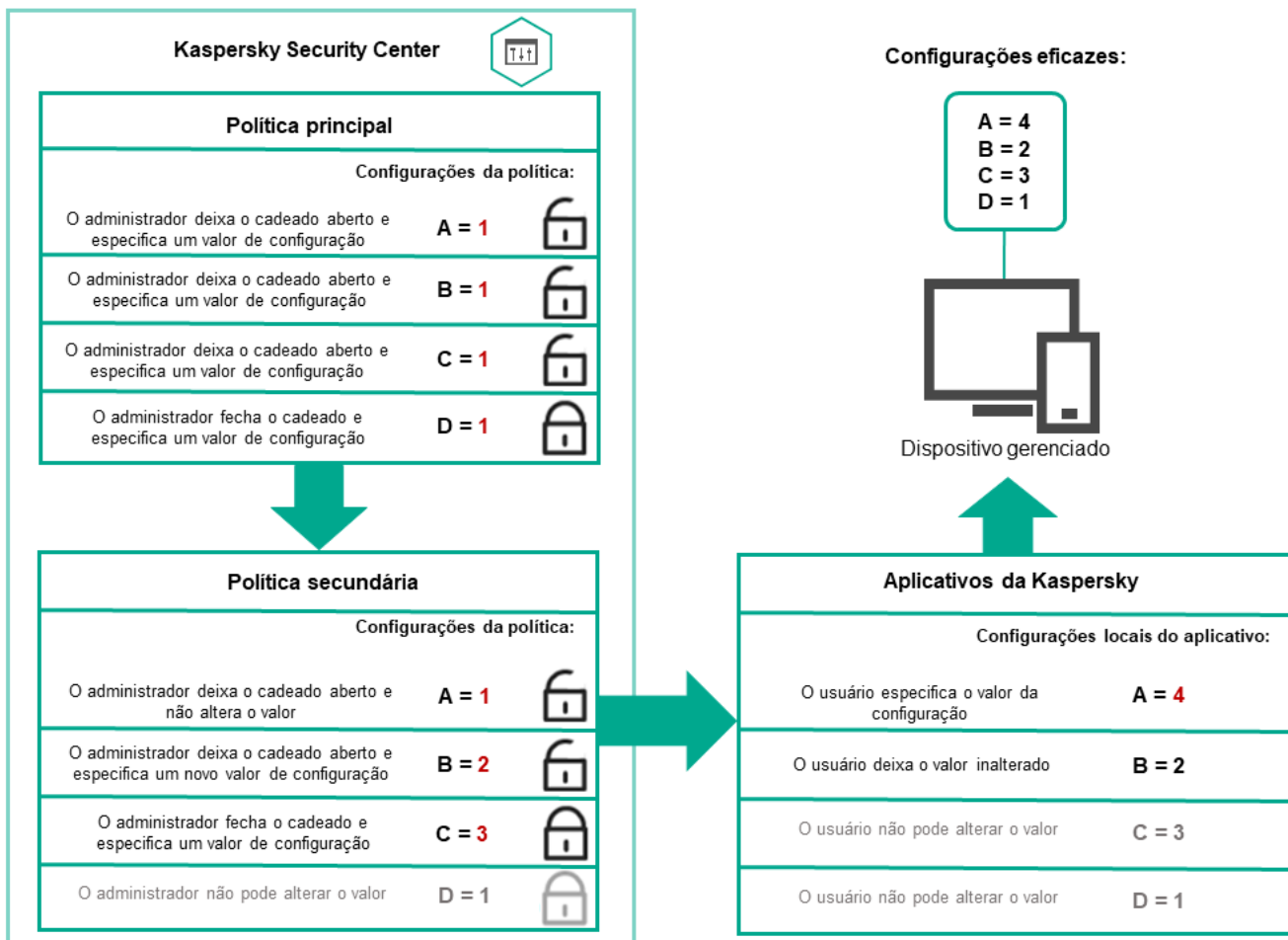
Se dispositivos diferentes precisarem de configurações diferentes, você pode organizar os dispositivos em grupos de administração.

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).

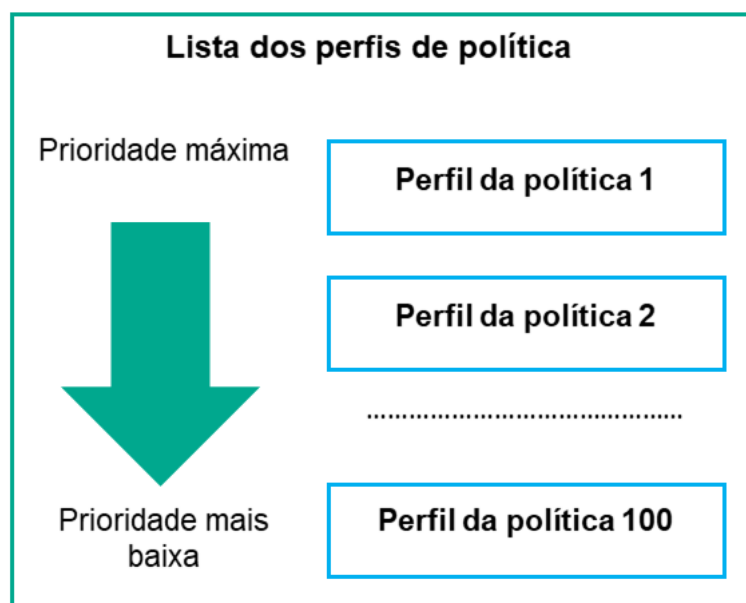


Hierarquia de políticas

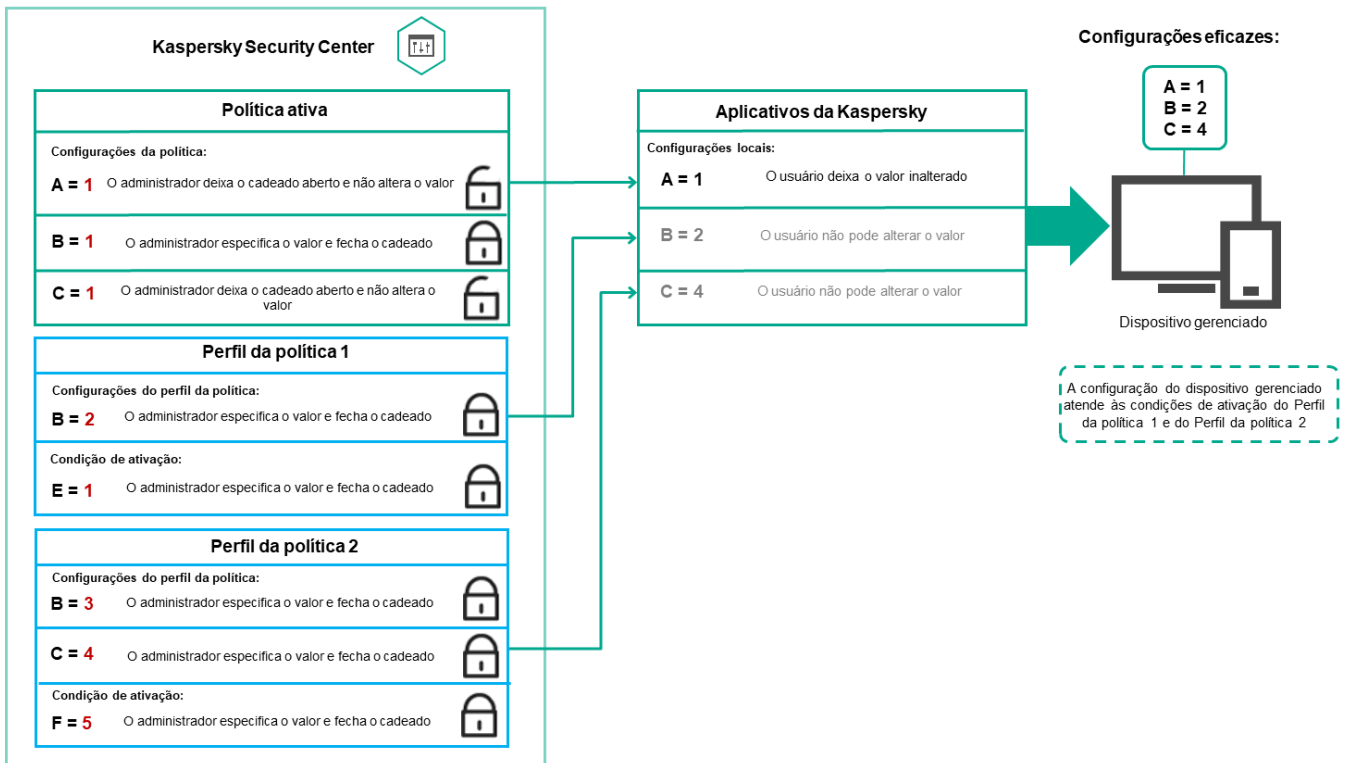
Perfis de política em uma hierarquia de políticas

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).

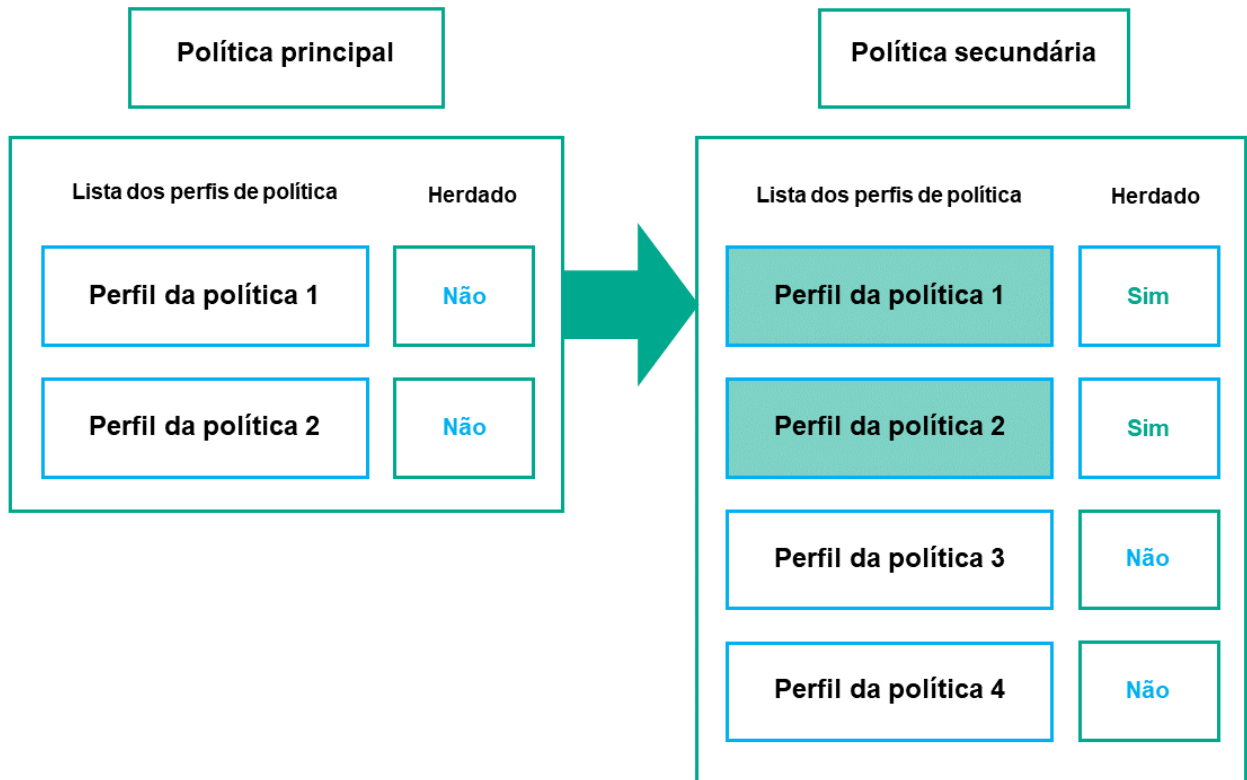


A configuração do dispositivo gerenciado atende às condições de ativação de vários perfis de política

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).

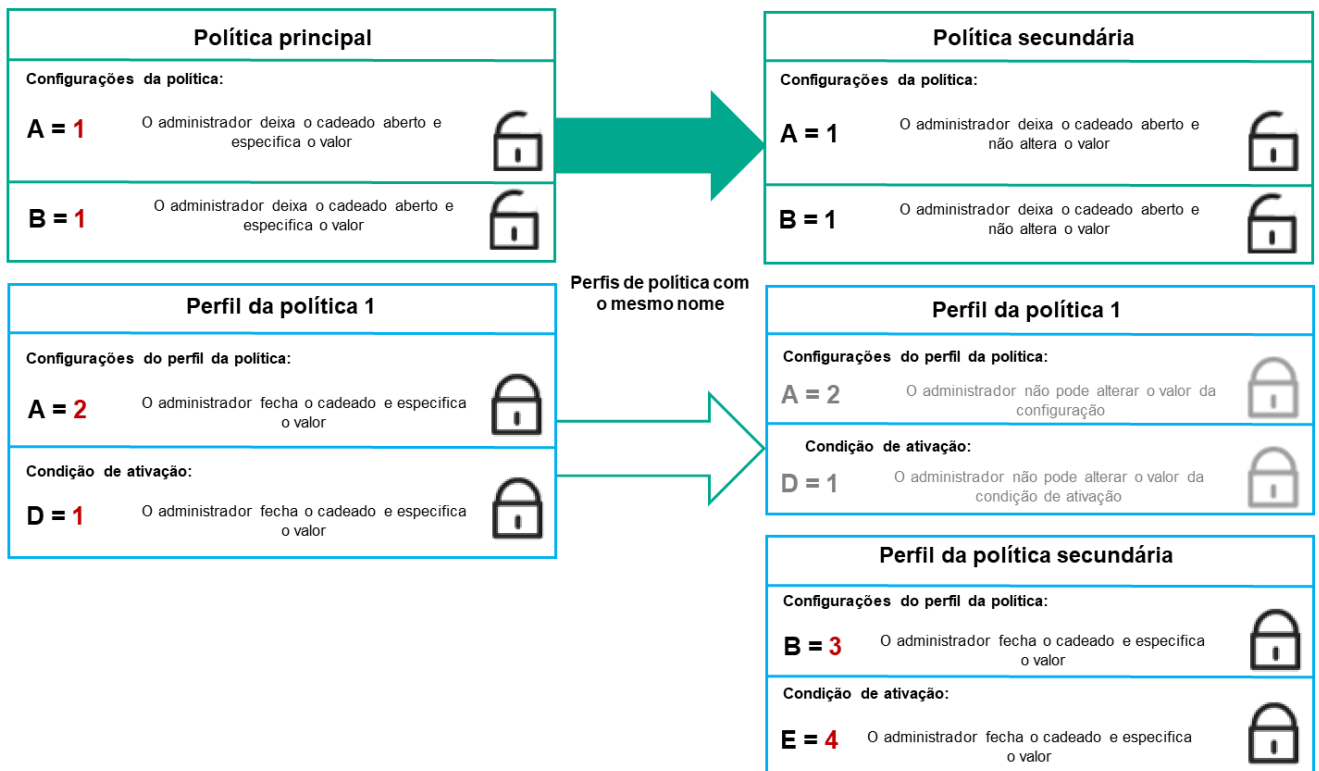


Herança de perfis de política

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 **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.

Para criar uma política:

1. Acesse **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. Selecione a 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).

O conjunto de configurações depende do aplicativo para o qual você cria uma política. Para mais detalhes, consulte:

- [Configuração do Servidor de Administração](#)
- [Configurações de política do Agente de Rede](#)
- [Ajuda do Kaspersky Endpoint Security for Linux](#) 

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.

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](#) [?]

Se esta opção estiver selecionada, a política é habilitada.
Por padrão, esta opção está selecionada.

- [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 grupos de administração aninhados, 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

Na guia **Configuração de eventos**, configure 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:

- **Exportar para o sistema SIEM usando o Syslog**
- **Armazenar no log de eventos do SO no dispositivo**
- **Armazenar no log de eventos do SO no Servidor de Administração**

- **Notificações de eventos**

Você pode selecionar se deseja ser notificado sobre o evento de uma das seguintes formas:

- **Notificar por e-mail**
- **Notificar por SMS**
- **Notificar ao executar o arquivo executável ou o script**
- **Notificar via SNMP**

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**, **SMS** e **Arquivo executável a ser executado**.

Histórico de revisões

A guia **Histórico de revisões** permite exibir a lista das revisões de política e [reverter alterações](#) feitas na política, se necessário.

Modificar uma política

Para modificar uma política:

1. Acesse **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](#)
- [Ajuda do Kaspersky Endpoint Security for Linux](#) ²

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**.

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 **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 **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).

Sincronização forçada

Embora o Kaspersky Security Center Linux automaticamente sincronize o status, configurações, tarefas e políticas para dispositivos gerenciados, em alguns casos, o administrador precisa saber exatamente, em um dado momento, 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. Acesse **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:
 - Vá para **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 uma política de um aplicativo da Kaspersky no Servidor de Administração, o administrador pode 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. Acesse **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 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.

Visualizar o gráfico de status de distribuição da política

No Kaspersky Security Center, você pode ver o status de aplicação da política em cada dispositivo através de um gráfico de status de distribuição de política.

Para analisar o status de distribuição da política em cada dispositivo:

1. Acesse **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 do status** 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. Acesse a seção **Opções da interface** na barra de ferramentas.

2. Em **Limite de dispositivos exibidos nos resultados de distribuição da política**, 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.

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 excluí-la no grupo de nível superior para o qual ela foi criada.

Para excluir uma política:

1. No menu principal, vá para **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 da política e fornece informações sobre como visualizá-los, alterar a prioridade, criar, 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 **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 da política**.

A lista de perfis da política é exibida em formato tabular. Se a política não tiver perfis, será exibida uma tabela vazia.

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 da 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 **Despriorizar**.

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 da 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.

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 da 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 da 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 "#").

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 Linux. 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 "#").

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 Linux. 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 menor 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 de 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:

- [Lista de tags](#) ?

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.

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 da 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.

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 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. Você pode 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.

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 Linux fornece meios de acesso baseado em função para os recursos do Kaspersky Security Center Linux e aplicativos gerenciados da Kaspersky.

Você pode configurar os [direitos de acesso aos recursos do aplicativo](#) para usuários do Kaspersky Security Center Linux 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 respectivas. 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 mostra os recursos do Kaspersky Security Center Linux com os direitos de acesso para gerenciar as tarefas, relatórios e configurações associadas, bem como executar as ações do usuário associadas.

Para executar as ações do usuário listadas na tabela, o usuário deve ter o direito especificado ao lado da ação.

Os direitos de **Ler**, **Modificar** e **Executar** 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	Modificar	<ul style="list-style-type: none"> • Adicionar dispositivo a um grupo de administração: Modificar • Excluir dispositivo de um grupo de administração: Modificar • Adicionar um grupo de administração a outro grupo de administração: Modificar • Excluir um grupo de administração de 	Nenhum	Nenhum

		outro grupo de administração: Modificar		
Recursos gerais: Acessar objetos independentemente de suas ACLs	Ler	Obter acesso de leitura a todos os objetos: Leitura	Nenhum	Nenhum
Recursos gerais: Funcionalidade básica	<ul style="list-style-type: none"> • Ler • Modificar • Executar • Executar operações nas seleções de dispositivos 	<ul style="list-style-type: none"> • Regras de migração de dispositivos (criar, modificar ou excluir) para o Servidor virtual: Modificar, 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: Modificar • Ver lista de controle de acesso de grupos: Ler • Ver o log de eventos Kaspersky: Leia 	<ul style="list-style-type: none"> • "Baixar atualizações no repositório do Servidor de Administração" • "Entregar relatórios" • "Distribuir pacote de instalação" • "Instalar aplicativos nos Servidores de Administração secundários remotamente" 	<ul style="list-style-type: none"> • "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 defesa de perímetro instalados" • "Relatório resumido dos tipos de aplicativos instalados" • "Relatório de usuários de dispositivos infectados" • "Relatório de incidentes" • "Relatório de eventos"

				<ul style="list-style-type: none"> • "Relatório de atividade dos pontos de distribuição" • "Relatório de Servidores de Administração secundários" • "Relatório de eventos de Controle de Dispositivos" • "Relatório de aplicativos proibidos" • "Relatório de Controle da Web" • "Relatório de permissões do usuário em vigor" • "Relatório de direitos"
Recursos gerais: Objetos excluídos	<ul style="list-style-type: none"> • Ler • Modificar 	<ul style="list-style-type: none"> • Ver os objetos excluídos na Lixeira: Ler • Excluir objetos da Lixeira: Modificar 	Nenhum	Nenhum
Recursos gerais: Processamento de eventos	<ul style="list-style-type: none"> • Excluir eventos • Editar configurações de notificação de eventos • Alterar configurações de log de eventos • Modificar 	<ul style="list-style-type: none"> • 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:
Operações no
Servidor de
Administração

- Ler
- Modificar
- Executar
- Modificar ACLs de objetos
- Executar operações nas seleções de dispositivos

- Especificar as portas do Servidor de Administração para a conexão do agente de rede:
Modificar
- Especificar as portas do Proxy de Ativação iniciado no Servidor de Administração:
Modificar
- Especificar as portas do Proxy de Ativação para Celular iniciado no Servidor de Administração:
Modificar
- Especificar as portas do Servidor Web para distribuição de pacotes autônomos:
Modificar
- Especificar as portas do Servidor Web para distribuição de perfis MDM:
Modificar
- Especificar as portas SSL do Servidor de Administração para conexão via Web Console: **Modificar**
- Especificar as portas do Servidor de Administração para conexão móvel:
Modificar
- Especificar o número máximo de eventos armazenados no banco de dados do Servidor de Administração:
Modificar

- "Backup de dados do Servidor de Administração"
- "Manutenção do banco de dados"

Nenhum

		<ul style="list-style-type: none"> • Especificar o número máximo de eventos que pode ser enviado pelo Servidor de Administração: Modificar • Especificar o período de tempo durante o qual os eventos podem ser enviados pelo Servidor de Administração: Modificar 		
Recursos gerais: Implementação de software da Kaspersky	<ul style="list-style-type: none"> • Gerenciar patches da Kaspersky • Ler • Modificar • Executar • Executar operações nas seleções de dispositivos 	Aprovar ou recusar a instalação do patch: Gerenciar patches da Kaspersky	Nenhum	<ul style="list-style-type: none"> • "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	<ul style="list-style-type: none"> • Exportar arquivo de chave • Modificar 	<ul style="list-style-type: none"> • Exportar arquivo de chave: Exportar arquivo de chave • Modificar as configurações de chave de licença do Servidor de Administração: Modificar 	Nenhum	Nenhum
Recursos gerais:			Nenhum	Nenhum

gerenciamento de relatórios aplicado	<ul style="list-style-type: none"> • Ler • Modificar 	<ul style="list-style-type: none"> • Criar relatórios independentemente 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Gerenciar Servidores de Administração virtuais • Ler • Modificar • Executar 	<ul style="list-style-type: none"> • Obter uma lista de Servidores de Administração virtuais: Ler • Obter informações sobre o Servidor de Administração virtual: Ler 	Nenhum	Nenhum

	<ul style="list-style-type: none"> • Executar operações nas seleções de dispositivos 	<ul style="list-style-type: none"> • Criar, atualizar ou excluir um Servidor de Administração virtual: Gerenciar Servidores de 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 		
--	---	---	--	--

Funções de usuário predefinidas

As funções de usuário atribuídas aos usuários do Kaspersky Security Center Linux fornecem conjuntos de direitos de acesso aos recursos do 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. Algumas das funções de usuário predefinidas disponíveis no Kaspersky Security Center Linux podem ser associadas a cargos específicos, por exemplo, **Auditor**, **Técnico de segurança**, **Supervisor**. 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 Ler e Modificar 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.

Características das áreas funcionais **Gerenciamento de dispositivos móveis: geral** e **Administração de sistema** não estão disponíveis no Kaspersky Security Center Linux. Um usuário com as funções **Administrador de Gerenciamento de Patches e Vulnerabilidades/Operador**, e **Administrador do Gerenciamento de Dispositivos Móveis/Operador** têm acesso apenas aos direitos de **Características gerais: área funcional Básica**.

Direitos de acesso de funções de usuário predefinidas

Função	Descrição
Administrador do Servidor de Administração	Permite todas as operações nas seguintes áreas funcionais, em Recursos gerais : <ul style="list-style-type: none"> • Funcionalidade básica • Processamento de eventos • Hierarquia de Servidores de Administração • Servidores de Administração virtual
Operador do Servidor de Administração	Concede os direitos de Ler e Executar em todas as seguintes áreas funcionais, nos Recursos gerais : <ul style="list-style-type: none"> • Funcionalidade básica • Servidores de Administração virtual
Auditor	Permite todas as operações nas seguintes áreas funcionais, em Recursos gerais : <ul style="list-style-type: none"> • Acessar objetos independentemente de suas ACLs • Objetos excluídos • Gerenciamento de relatórios aplicado <p>Você pode atribuir esta função a uma pessoa que realiza a auditoria da sua organização.</p>
Administrador de instalação	Permite todas as operações nas seguintes áreas funcionais, em Recursos gerais : <ul style="list-style-type: none"> • Funcionalidade básica • Implementação de software da Kaspersky • Gerenciamento de chaves de licença <p>Concede os direitos de Ler e Executar na área funcional Recursos gerais: Servidores de Administração Virtuais.</p>
Operador de instalação	Concede os direitos de Ler e Executar em todas as seguintes áreas funcionais, nos Recursos gerais : <ul style="list-style-type: none"> • Funcionalidade básica • Implementação de software da Kaspersky (também concede o direito de Gerenciar patches da Kaspersky Lab nesta área) • Servidores de Administração virtual
Administrador do	Permite todas as operações nas seguintes áreas funcionais:

Kaspersky Endpoint Security	<ul style="list-style-type: none"> • Recursos gerais: Funcionalidade básica • Área do Kaspersky Endpoint Security, incluindo todos os recursos
Operador do Kaspersky Endpoint Security	<p>Concede os direitos de Ler e Executar em todas as seguintes áreas funcionais:</p> <ul style="list-style-type: none"> • Recursos gerais: Funcionalidade básica • Área do Kaspersky Endpoint Security, incluindo todos os recursos
Administrador Principal	<p>Permite todas as operações em áreas funcionais, <i>exceto</i> as seguintes áreas, em Recursos gerais:</p> <ul style="list-style-type: none"> • Acessar objetos independentemente de suas ACLs • Gerenciamento de relatórios aplicado
Operador Principal	<p>Concede os direitos de Ler e Executar (quando aplicável) em todas as seguintes áreas funcionais:</p> <ul style="list-style-type: none"> • Recursos gerais: • Funcionalidade básica • Objetos excluídos • Operações no Servidor de Administração • Implementação de software da Kaspersky Lab • Servidores de Administração virtual • Área do Kaspersky Endpoint Security, incluindo todos os recursos
Administrador do Gerenciamento de Dispositivos Móveis	<p>Permite todas as operações na área funcional Recursos gerais: Funcionalidade básica.</p>
Diretor de segurança	<p>Permite todas as operações nas seguintes áreas funcionais, em Recursos gerais:</p> <ul style="list-style-type: none"> • Acessar objetos independentemente de suas ACLs • Gerenciamento de relatórios aplicado <p>Concede os direitos de Ler, Modificar, Executar, Salvar os arquivos dos dispositivos na estação de trabalho do administrador e Executar operações nas seleções de dispositivos na área funcional Gerenciamento do sistema: Conectividade.</p> <p>Você pode atribuir esta função a um diretor responsável pela segurança de TI em sua organização.</p>
Usuário do Self Service Portal	<p>Permite todas as operações na área funcional Gerenciamento de Dispositivos Móveis: Self Service Portal. Este recurso não é compatível com o Kaspersky Security Center 11 e versões posteriores.</p>
Supervisor	<p>Concede o direito de Ler nas áreas funcionais Recursos gerais: Acessar objetos independentemente de suas ACLs e Recursos gerais: Gerenciamento de relatórios</p>

aplicado.

Você pode atribuir esta função a um diretor de segurança e a outros gerentes responsáveis pela segurança de TI em sua organização.

Adicionar uma conta de usuário interno

Para adicionar uma nova conta de usuário interno ao Kaspersky Security Center Linux:

1. No menu principal, vá para **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**.
2. Clique em **Adicionar**.
3. Na janela **Nova entidade** que se abre, especifique as configurações da conta do novo usuário:

- Mantenha a opção padrão **Usuário**.
- **Nome**.
- **Senha** para a conexão do usuário ao Kaspersky Security Center Linux.
A senha deve estar em conformidade com as seguintes regras:
 - A senha deve ter de 8 a 16 caracteres.
 - A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
 - Letras maiúsculas (A-Z)
 - Letras minúsculas (a-z)
 - Números (0-9)
 - Caracteres especiais (@ # \$ % ^ & * - _ ! + = [] { } | : ' . ? / \ ` ~ " () ;)
 - A senha não deve conter nenhum espaço em branco, caracteres Unicode ou a combinação dos caracteres "." e "@", quando "." estiver colocado antes de "@".

Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

O número de tentativas de entrada da senha é limitado. Por padrão, o número máximo de tentativas permitidas de entrada da senha é de 10. Você pode modificar o número permitido de tentativas de inserção de senha, como descrito em ["Alterar o número permitido de tentativas de entrada de senha"](#).

Se o usuário inserir uma senha inválida no número especificado de vezes, a conta do usuário é bloqueada por um hora. Você pode desbloquear a conta do usuário somente ao alterar a senha.

- **Nome completo**
- **Descrição**
- **Endereço de e-mail**

- **Telefone**

4. Clique em **OK** para salvar as alterações.

A nova conta de usuário aparece na lista de grupos de usuários e usuários.

Criar um grupo de usuários

Para criar um grupo de usuários:

1. No menu principal, vá para **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**.
2. Clique em **Adicionar**.
3. Na janela que se abre **Nova entidade**, selecione **Grupo**.
4. Especifique as seguintes configurações para o novo grupo de usuários:

- **Nome do grupo**
- **Descrição**

5. Clique em **OK** para salvar as alterações.

O novo grupo de usuários aparece na lista de grupos de usuários e usuários.

Editar uma conta de usuário interno

Para editar uma nova conta de usuário interno ao Kaspersky Security Center Linux:

1. No menu principal, vá para **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**.
2. Clique no nome da conta de usuário que deseja editar.
3. Na janela de configurações do usuário exibida, na guia **Geral**, altere as configurações da conta de usuário:

- **Descrição**
- **Nome completo**
- **Endereço de e-mail**
- **Telefone principal**
- **Senha** para a conexão do usuário ao Kaspersky Security Center Linux.

A senha deve estar em conformidade com as seguintes regras:

- A senha deve ter de 8 a 16 caracteres.

- A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
 - Letras maiúsculas (A-Z)
 - Letras minúsculas (a-z)
 - Números (0-9)
 - Caracteres especiais (@ # \$ % ^ & * - _ ! + = [] { } | : ' . , ? / \ ` ~ " () ;)
- A senha não deve conter nenhum espaço em branco, caracteres Unicode ou a combinação dos caracteres "." e "@", quando "." estiver colocado antes de "@".

Para ver a senha inserida, mantenha pressionado o botão **Exibir**.

O número de tentativas de entrada da senha é limitado. Por padrão, o número máximo de tentativas permitidas de entrada da senha é de 10. É possível [alterar](#) o número permitido de tentativas; no entanto, por motivos de segurança, não recomendamos diminuir esse número. Se o usuário inserir uma senha inválida no número especificado de vezes, a conta do usuário é bloqueada por um hora. Você pode desbloquear a conta do usuário somente ao alterar a senha.

- Se necessário, mude o botão de alternar para **Desativado** para impedir o usuário de se conectar ao aplicativo. Você pode desativar uma conta, por exemplo, depois que um funcionário sai da empresa.
4. Na guia **Segurança de autenticação**, você pode especificar as configurações de segurança para esta conta.
 5. Na guia **Grupos**, você pode adicionar o usuário a grupos de segurança.
 6. Na guia **Dispositivos**, você pode [atribuir dispositivos](#) ao usuário.
 7. Na guia **Funções**, você pode [atribuir funções](#) ao usuário.
 8. Clique em **Salvar** para salvar as alterações.

A conta de usuário atualizada aparece na lista de grupos de segurança e usuários.

Editar um grupo de usuários

Você pode editar apenas grupos internos.

Para editar um grupo de usuários:

1. No menu principal, vá para **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**.
2. Clique no nome do grupo de usuários que deseja editar.
3. Na janela de propriedades do grupo que se abre, altere as configurações do grupo de usuários:
 - **Nome**

- **Descrição**

4. Clique em **Salvar** para salvar as alterações.

O grupo de usuários atualizado aparece na lista de grupos de usuários e usuários.

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**.
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.

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. No menu principal, vá para **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**.
2. Clique no nome da conta de usuário que deseja atribuir como proprietário do dispositivo.
3. Na janela aberta de configurações do usuário, clique na guia **Dispositivos**.
4. Clique em **Adicionar**.
5. Na lista de dispositivos, selecione o dispositivo que deseja atribuir ao usuário.
6. Clique em **OK**.

O dispositivo selecionado é adicionado à lista de dispositivos atribuídos ao usuário.

Você pode executar a mesma operação em **DISPOSITIVOS** → **DISPOSITIVOS GERENCIADOS**, clicando no nome do dispositivo que deseja atribuir e clicando no link **Gerenciar proprietário do dispositivo**.

Excluir um usuário ou um grupo de segurança

Você pode excluir apenas usuários internos ou grupos de segurança internos.

Para excluir um usuário ou um grupo de segurança:

1. No menu principal, vá para **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**.
2. Marque a caixa de seleção ao lado do usuário ou do grupo de segurança que deseja excluir.
3. Clique em **Excluir**.
4. Na janela que se abre, clique em **OK**.

O usuário ou o grupo de segurança é excluído.

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 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 segurança 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**.
2. Marque as caixas de seleção ao lado dos usuários e grupos de segurança 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 o Assistente.

Os usuários ou os grupos de segurança 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 segurança que deseja adicionar ao escopo da função de usuário.
7. Clique no botão **Atribuir função** para fechar o Assistente.
8. Clique no botão **Fechar** (X) para fechar a janela de propriedades da função.

Os usuários ou os grupos de segurança 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.

Gerenciar revisões de objeto

Esta seção contém informações sobre o gerenciamento de revisão de objeto. O Kaspersky Security Center Linux lhe permite acompanhar a modificação de objeto. Cada vez quando você salva modificações feitas à um objeto, uma *revisão* é criada. Cada revisão tem um número.

Os objetos do aplicativo suportam o gerenciamento de revisão incluem:

- Servidores de Administração
- Políticas
- Tarefas
- Grupos de administração
- Contas de usuário
- Pacotes de instalação

Você pode executar as seguintes ações nas revisões do objeto:

- Comparar uma revisão selecionada à atual
- Comparar as revisões selecionadas
- Comparar um objeto com uma revisão selecionada de outro objeto do mesmo tipo
- Exibir uma revisão selecionada
- Reverter as modificações feitas a um objeto para uma revisão selecionada
- Salve as revisões como um arquivo .txt

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 **Descrição**. Na janela **Descrição da revisão do objeto**, insira algum texto para a descrição da revisão.

Sobre as revisões do objeto

Você pode executar as seguintes ações nas revisões do objeto:

- Comparar uma revisão selecionada à atual
- Comparar as revisões selecionadas
- Comparar um objeto com uma revisão selecionada de outro objeto do mesmo tipo
- Exibir uma revisão selecionada
- Reverter as modificações feitas a um objeto para uma revisão selecionada
- Salve as revisões como um arquivo .txt

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

Reverter um objeto para uma revisão anterior

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. Na janela de propriedades do objeto, abra a guia **Histórico de revisões**.
2. Na lista de revisões do objeto, selecione a revisão para a qual você precisa reverter as modificações.
3. Clique no botão **Reverter**.
4. Clique em **OK** para confirmar a operação.

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.

A operação de reversão está disponível apenas para objetos de política e tarefa.

Exclusão de objetos

Esta seção fornece informações sobre como excluir objetos e como exibir as informações sobre os objetos após a sua exclusão.

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**.

Usando o utilitário klscflag para abrir a porta 13291

A porta 13291 do Servidor de Administração é usada para receber conexões dos Consoles de Administração. Em computadores que não rodam o Windows, esta porta não está aberta por padrão. Para usar o Console de Administração baseado em MMC ou o utilitário klakaut, é possível abrir essa porta usando o utilitário klscflag. Este utilitário altera o valor do parâmetro KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Para abrir a porta 13291:

1. Execute o seguinte comando na linha de comando:

```
$ klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

2. Reinicie o serviço do Servidor de Administração do Kaspersky Security Center executando o seguinte comando:

```
$ sudo systemctl restart kladminserver_srv
```

A porta 13291 está aberta.

Para verificar se a porta 13291 foi aberta com êxito:

Execute o seguinte comando na linha de comando:

```
$ klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

Este comando retorna o seguinte resultado:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T>true
```

O valor verdadeiro significa que a porta está aberta. Caso contrário, o valor falso é exibido.

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

Cenário: Atualização regular dos bancos de dados e dos aplicativos Kaspersky

Esta seção fornece um cenário para a atualização regular de bancos de dados, módulos de software e aplicativos da Kaspersky. Após ter concluído o [Cenário de configuração de proteção da rede](#), você precisará manter a confiabilidade do sistema de proteção para ter certeza de que os Servidores de Administração e os dispositivos gerenciados estejam permanentemente protegidos contra várias ameaças, incluindo vírus, ataques à rede e ataques de phishing.

A proteção da rede é mantida atualizada por atualizações regulares dos seguintes:

- Bancos de dados e módulos de software da Kaspersky
- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center

Quando concluir este cenário, você poderá ter certeza do seguinte:

- A sua rede está protegida pelo software da Kaspersky mais recente, inclusive aplicativos de segurança e componentes do Kaspersky Security Center Linux.
- Os bancos de dados de antivírus e outros bancos de dados da Kaspersky críticos para a segurança de rede são sempre atualizados

Pré-requisitos

Os dispositivos gerenciados devem ter uma conexão com o Servidor de Administração. Se eles não tiverem uma conexão, considere [atualizar os bancos de dados da Kaspersky e módulos do software manualmente](#) ou [diretamente dos servidores de atualização da Kaspersky](#).

O Servidor de Administração deve ter uma conexão com a Internet.

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

1. Implementado os aplicativos de segurança da Kaspersky nos dispositivos gerenciados de acordo com o [cenário de implementação de aplicativos da Kaspersky através do Kaspersky Security Center 14 Web Console](#).
2. Criado e configurado todos os perfis da política, políticas e tarefas necessários segundo o [cenário de configuração da proteção de rede](#).
3. [Atribuído um volume apropriado de pontos de distribuição](#) conforme o número de dispositivos gerenciados e a topologia de rede.

A atualização dos bancos de dados e dos aplicativos da Kaspersky prossegue em estágios:

1 Seleção de um esquema de atualização

Há [vários esquemas](#) que você pode usar para instalar atualizações para componentes e aplicativos de segurança do Kaspersky Security Center. Selecione o esquema ou vários esquemas que atendem aos requisitos de sua melhor rede.

2 Criar a tarefa para baixar as atualizações no repositório do Servidor de Administração

Essa tarefa é criada automaticamente pelo Assistente de Início Rápido do Kaspersky Security Center. Se você não tiver executado o Assistente, crie a tarefa agora.

Essa tarefa é necessária para baixar atualizações de servidores de atualização da Kaspersky para o repositório do Servidor de Administração, bem como atualizar bancos de dados e módulos do software da Kaspersky para o Kaspersky Security Center. Após o download das atualizações, elas podem ser propagadas aos dispositivos gerenciados.

Se a rede tiver pontos de distribuição atribuídos, as atualizações serão baixadas automaticamente do repositório do Servidor de Administração para os repositórios dos pontos de distribuição. Nesse caso, os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição em vez de do repositório do Servidor de Administração.

Instruções: [Como criar a tarefa para baixar as atualizações para o repositório do Servidor de Administração](#)

3 Criar a tarefa para baixar as atualizações para os repositórios de pontos de distribuição (opcional)

Por padrão, as atualizações são baixadas para os pontos de distribuição do Servidor de Administração. Você pode configurar o Kaspersky Security Center para baixar as atualizações para os pontos de distribuição diretamente dos servidores de atualização da Kaspersky. Faça o download para os repositórios dos pontos de distribuição se o tráfego entre o Servidor de Administração e os pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.

Quando a rede tiver atribuído pontos de distribuição e a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for criada, os pontos de distribuição baixarão atualizações dos servidores de atualização da Kaspersky e não do repositório do Servidor de Administração.

Instruções de como proceder: [Como criar a tarefa para baixar atualizações nos repositórios dos pontos de distribuição](#)

4 Configurar os pontos de distribuição

Quando a sua rede tem pontos de distribuição atribuídos, certifique-se de que a opção **Implementar atualizações** esteja ativada nas propriedades de todos os pontos de distribuição necessários. Quando essa opção é desativada para um ponto de distribuição, os dispositivos incluídos no escopo das atualizações de download do ponto de distribuição do repositório do Servidor de Administração.

5 Como otimizar o processo de atualização usando os arquivos diff (opcional)

Você pode otimizar o tráfego entre o Servidor de Administração e os dispositivos gerenciados usando [arquivos diff](#). Quando esse recurso for ativado, o Servidor de Administração ou um ponto de distribuição baixará arquivos diff em vez de arquivos inteiros de bancos de dados ou módulos de software da Kaspersky. Um arquivo diff descreve as diferenças entre duas versões de um arquivo de banco de dados ou módulo de software. Por isso, um arquivo diff ocupa menos espaço do que um arquivo inteiro. Isso resulta na redução no tráfego entre o Servidor de Administração ou os pontos de distribuição e os dispositivos gerenciados. Para usar esse recurso, ative a opção **Baixar arquivos diff** nas propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e/ou 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](#)

6 Configuração da instalação automática de atualizações para os aplicativos de segurança

Crie a tarefa *Atualizar* para os aplicativos gerenciados para fornecer atualizações oportunas para os módulos do software e bancos de dados Kaspersky, inclusive bancos de dados de antivírus. Para assegurar atualizações oportunas, recomendamos selecionar a opção **Quando novas atualizações são baixadas no repositório** ao [configurar a programação de tarefa](#).

Se sua rede incluir somente dispositivos IPv6 e você deseja atualizar regularmente os aplicativos de segurança instalados neles, certifique-se de que o Servidor de Administração versão 13.2 e o Agente de Rede versão 13.2 estejam instalados nos dispositivos gerenciados.

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.

Resultados

Após a conclusão do cenário, o Kaspersky Security Center Linux é configurado para atualizar os bancos de dados da Kaspersky após as atualizações serem baixadas para o repositório do Servidor de Administração. Você poderá prosseguir para monitorar o 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 Servidores de Administração e dispositivos gerenciados esteja atualizada, você deverá fornecer atualizações oportunas dos seguintes:

- 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 verifica se os servidores da Kaspersky estão acessíveis. Se não for possível acessar os servidores usando o DNS do sistema, o aplicativo usa o DNS público. 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

Kaspersky Security Center não pode atualizar os aplicativos Kaspersky automaticamente. Para atualizar os aplicativos, baixe as versões mais recentes do aplicativo no site da Kaspersky e instale-as manualmente:

- [Servidor de Administração do Kaspersky Security Center, Kaspersky Security Center 14 Web Console](#) 
- [Agente de rede, Kaspersky Endpoint Security for Linux, plugin de gerenciamento da web](#) 

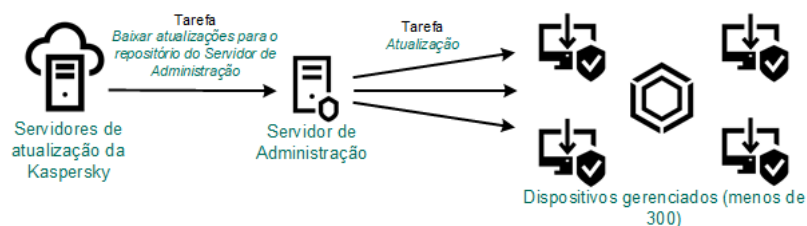
Dependendo da configuração da rede, você pode usar os seguintes esquemas de download e distribuição das atualizações necessárias para os dispositivos gerenciados:

- Usando uma única tarefa: *Baixar atualizações no repositório do Servidor de Administração*
- Usando duas tarefas:
 - A tarefa *Baixar atualizações no repositório do Servidor de Administração*
 - A 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 o Kaspersky Endpoint Security for Linux nos dispositivos gerenciados
- Por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

Usando a tarefa Baixar atualizações no repositório do Servidor de Administração

Nesse esquema, o Kaspersky Security Center baixa as atualizações através da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Em redes pequenas que contêm menos de 300 dispositivos gerenciados em um segmento de rede único ou menos de 10 dispositivos gerenciados em cada segmento de rede, as atualizações são distribuídas aos dispositivos gerenciados diretamente do repositório do Servidor de Administração (veja a figura abaixo).



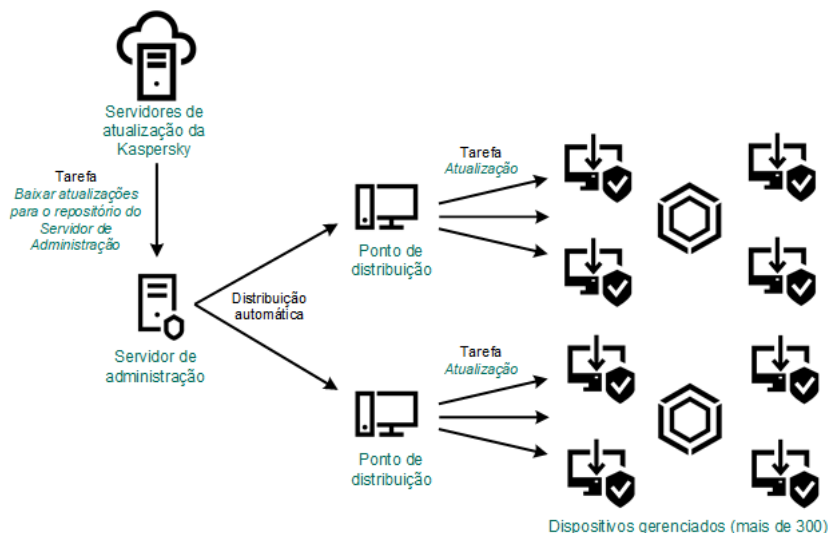
Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração sem pontos de distribuição

Como uma [fonte de atualizações](#), é possível usar não somente os servidores de atualização Kaspersky, mas também uma pasta local ou de rede.

Por padrão, o Servidor de Administração comunica-se com os servidores de atualização Kaspersky e baixa as atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração para usar o protocolo HTTP em vez de HTTPS.

Se a rede contiver 300 dispositivos gerenciados ou mais em um segmento de rede único ou se a rede consistir em vários segmentos de rede com mais de 9 dispositivos gerenciados em cada segmento de rede, recomendamos o uso de pontos de distribuição para propagar as atualizações aos dispositivos gerenciados (veja a figura abaixo). Os pontos de distribuição reduzem a carga no Servidor de Administração e otimizam o tráfego entre o Servidor de Administração e os dispositivos gerenciados. Você pode [calcular](#) o número e a configuração de pontos de distribuição necessários para a rede.

Nesse esquema, as atualizações são baixadas automaticamente do repositório do Servidor de Administração para os repositórios dos pontos de distribuição. Os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição em vez de do repositório do Servidor de Administração.



Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração com pontos de distribuição

Quando o *Baixar atualizações no repositório do Servidor de Administração* estiver concluída, as atualizações dos bancos de dados Kaspersky e módulos de software do Kaspersky Endpoint Security for Linux são baixados para o repositório do Servidor de Administração. Essas atualizações são instaladas por meio da tarefa de Atualização para o Kaspersky Endpoint Security for Linux.

A tarefa *Baixar atualizações para o repositório do Servidor de Administração* não está disponível nos Servidores de Administração virtuais. O repositório do Servidor de Administração virtual exibe as atualizações baixadas para o Servidor de Administração principal.

Você pode configurar as atualizações a serem verificadas quanto a operabilidade e erros em um conjunto de dispositivos de teste. Se a verificação for bem-sucedida, as atualizações serão distribuídas para outros dispositivos gerenciados.

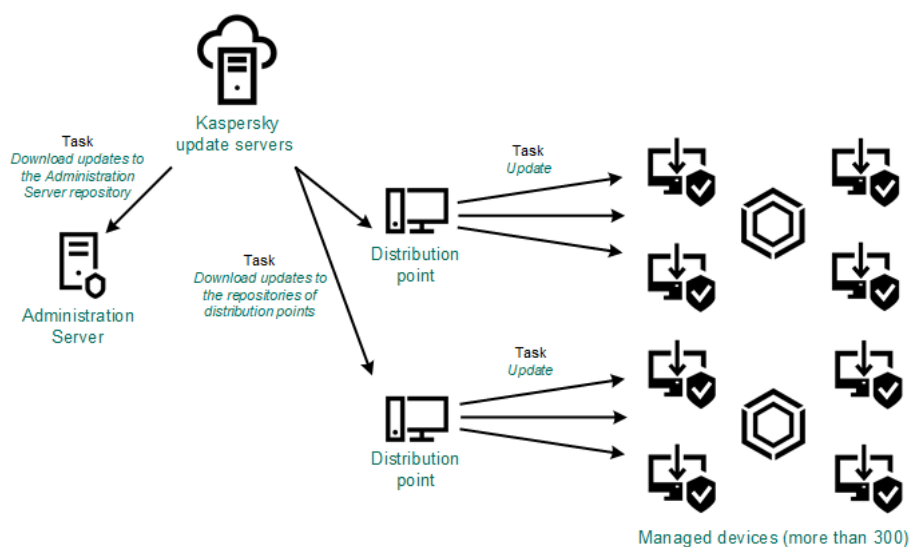
Cada aplicativo da Kaspersky solicita as atualizações necessárias do Servidor de Administração. O Servidor de Administração agrega essas solicitações e baixa somente as que são solicitadas por qualquer aplicativo. Isso garante que as mesmas atualizações não sejam baixadas várias vezes e impede que as atualizações desnecessárias sejam baixadas. Ao executar a tarefa *Baixar atualizações no repositório do Servidor de Administração*, 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 configuração do aplicativo
- ID da chave ativa
- ID de execução da tarefa *Baixar atualizações para o repositório do Servidor de Administração*

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.

Usando duas tarefas: a tarefa *Baixar atualizações no repositório do Servidor de Administração* e a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*

Você pode baixar atualizações para os repositórios de pontos de distribuição diretamente dos servidores de atualização Kaspersky em vez de do repositório do Servidor de Administração e distribuir as atualizações para os dispositivos gerenciados (veja a figura abaixo). Faça o download para os repositórios dos pontos de distribuição se o tráfego entre o Servidor de Administração e os pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.



Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração e a tarefa Baixar atualizações para os repositórios de pontos de distribuição

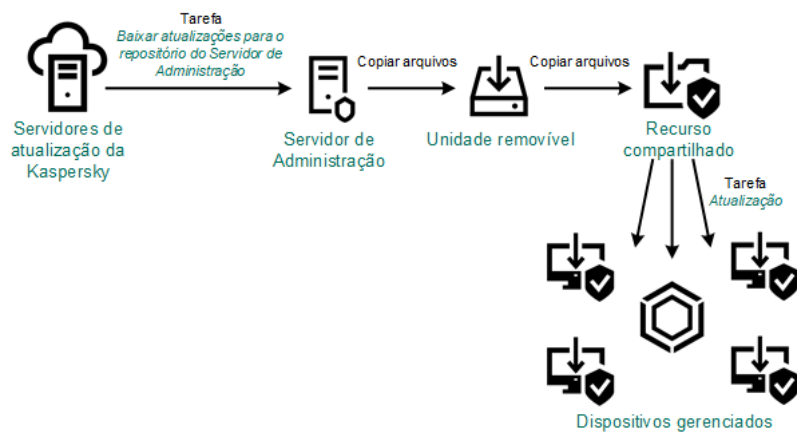
Por padrão, o Servidor de Administração e os pontos de distribuição comunicam-se com Servidores de atualização Kaspersky e baixam de atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração e/ou os pontos de distribuição para usar o protocolo HTTP em vez de HTTPS.

Para implementar esse esquema, crie a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* além da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Depois disso, os pontos de distribuição baixarão atualizações dos servidores de atualização Kaspersky e não do repositório do Servidor de Administração.

A tarefa *Baixar atualizações no repositório do Servidor de Administração* também é necessária para esse esquema, porque essa tarefa é usada para baixar módulos de software e bancos de dados da Kaspersky para o Kaspersky Security Center.

Manualmente por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP

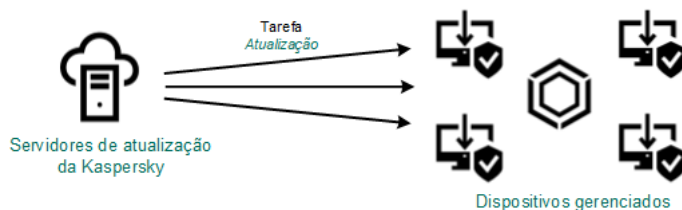
Se os dispositivos cliente não tiverem uma conexão com o Servidor de Administração, você poderá usar uma pasta local ou um recurso compartilhado como uma origem para [atualizar bancos de dados, módulos de software e aplicativos Kaspersky](#). Nesse esquema, você precisa copiar as atualizações necessárias do repositório do Servidor de Administração para uma unidade removível e depois copiar as atualizações para a pasta local ou o recurso compartilhado especificado como uma fonte de atualização nas configurações do [Kaspersky Endpoint Security for Linux](#) (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 Linux nos dispositivos gerenciados

Nos dispositivos gerenciados, você pode configurar o Kaspersky Endpoint Security for Linux 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 o repositório fornecido pelo Kaspersky Security Center. Para receber atualizações diretamente dos servidores de atualização da Kaspersky, especifique os servidores de atualização da Kaspersky como uma fonte de atualização no aplicativo de segurança. Para uma descrição completa dessas configurações, consulte a [documentação do Kaspersky Endpoint Security for Linux](#).

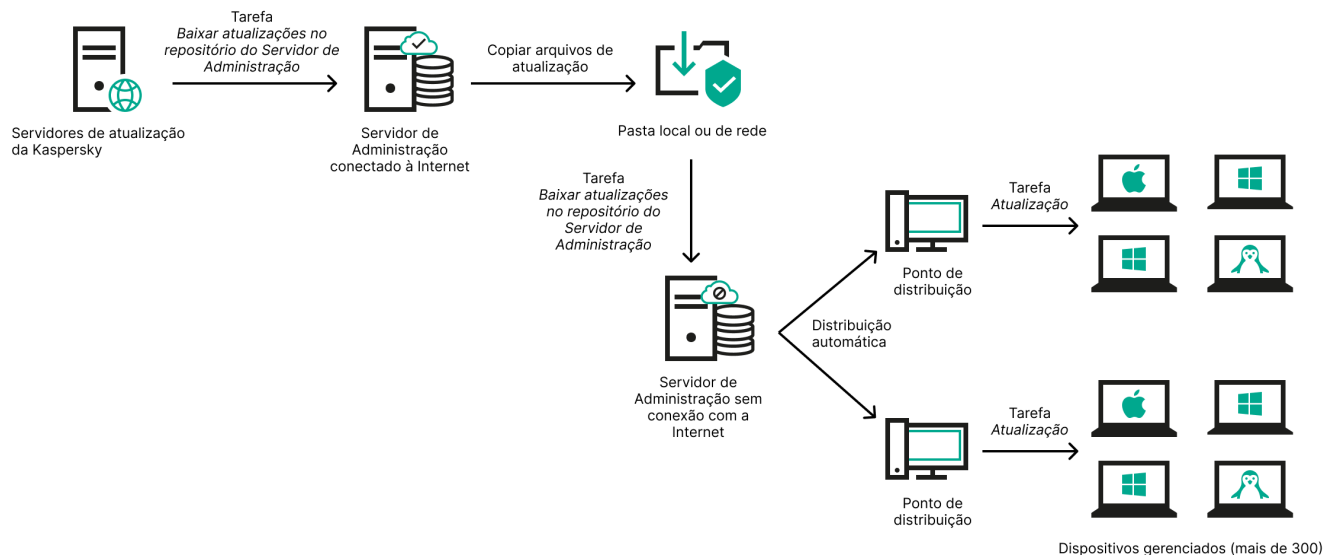
Por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

Se o Servidor de Administração não tiver conexão com a Internet, você poderá configurar a tarefa *Baixar atualizações no repositório do Servidor de Administração* para baixar atualizações de uma pasta local ou de rede. Nesse caso, você deve copiar os arquivos de atualização necessários para a pasta especificada de tempos em tempos. Por exemplo, você pode copiar os arquivos de atualização necessários de uma das seguintes fontes:

- Servidor de Administração que possui conexão com a Internet (veja a figura abaixo)

Como um Servidor de Administração baixa apenas as atualizações solicitadas pelos aplicativos de segurança, os conjuntos de aplicativos de segurança gerenciados pelos Servidores de Administração (o que tem conexão com a Internet e o que não tem) devem corresponder.

Se o Servidor de Administração que você usa para baixar atualizações tiver a versão 13.2 ou anterior, abra as propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e, em seguida, ative a opção **Baixar atualizações usando o esquema antigo**.



Atualização por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

- [Utilitário de atualização da Kaspersky](#)

Como este utilitário usa o esquema antigo para baixar atualizações, abra as propriedades da tarefa [Baixar atualizações no repositório do Servidor de Administração](#) e, em seguida, ative a opção *Baixar atualizações usando o esquema antigo*.

Criação da tarefa baixar atualizações no repositório do Servidor de Administração

A tarefa *Baixar atualizações no repositório do Servidor de Administração* permite baixar atualizações de bancos de dados e módulos de software do aplicativos de segurança do Kaspersky a partir dos servidores de atualização do Kaspersky para o repositório do Servidor de Administração.

O Assistente de Início Rápido do Kaspersky Security Center [cria automaticamente](#) a tarefa *Baixar atualizações no repositório do Servidor de Administração* do Servidor de Administração. Na lista de tarefas, só pode haver uma tarefa *Baixar atualizações no repositório do Servidor de Administração*. É possível criar esta tarefa novamente caso ela seja removida da lista de tarefas do Servidor de Administração.

Após a tarefa *Baixar atualizações no repositório do Servidor de Administração* ser concluída e as atualizações forem baixadas, elas poderão ser propagadas aos dispositivos gerenciados.

Antes de distribuir as atualizações para os dispositivos gerenciados, é possível executar a tarefa de [Verificação de atualizações](#). Isso permite ter a certeza de que o Servidor de Administração instalará as atualizações baixadas corretamente e que um nível de segurança não diminuirá devido às atualizações. Para verificá-las antes de distribuir, configure a opção **Executar verificação de atualizações** nas configurações de tarefas *Baixar atualizações no repositório do Servidor de Administração*.

Para criar uma tarefa *Baixar atualizações no repositório do Servidor de Administração*:

1. Acesse **DISPOSITIVOS** → **TAREFAS**.
2. Clique em **Adicionar**.
O Assistente para Novas Tarefas inicia. Siga as etapas do Assistente.

3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Baixar atualizações no repositório do 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. Na página **Concluir a criação da tarefa**, é possível ativar a opção **Abrir detalhes da tarefa quando a criação for concluída** para abrir a janela de propriedades da tarefa e modificar as configurações padrão da tarefa. Caso contrário, será possível definir as configurações da tarefa posteriormente, no momento oportuno.
6. Clique no botão **Concluir**.
A tarefa é criada e exibida na lista de tarefas.
7. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.
8. Na janela de propriedades da tarefa, na guia **Configurações do aplicativo**, especifique as seguintes configurações:

- **[Fontes de atualizações](#)**

Como uma [fonte de atualizações](#), é possível usar servidores de atualização da Kaspersky, uma pasta local ou de rede ou um Servidor de Administração principal.

- **[Pasta para armazenar atualizações](#)**

O caminho para a [pasta especificada](#) para armazenar as 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.

- **[Copiar as atualizações baixadas em pastas adicionais](#)**

Após recepção das atualizações pelo Servidor de Administração, estas são copiadas para as pastas especificadas. Use esta opção se você deseja gerenciar manualmente a distribuição das atualizações na rede.

Por exemplo, você pode desejar usar esta opção na seguinte situação: a rede de sua organização consiste em várias sub-redes independentes e os dispositivos de cada uma das sub-redes não têm acesso a outras sub-redes. Entretanto, os dispositivos em todas as sub-redes têm acesso a um compartilhamento de rede comum. Neste caso, você define o Servidor de Administração em uma das sub-redes para baixar atualizações dos Servidores de Atualização Kaspersky, ativar essa opção e especificar esse compartilhamento de rede. Nas atualizações baixadas para as tarefas de repositório de outros Servidores de Administração, especifique o mesmo compartilhamento de rede como a origem da atualização.

Por padrão, esta opção está desativada.

- **[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](#)**

A partir da versão 14, o Kaspersky Security Center baixa as atualizações de bancos de dados e os 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, o Servidor de Administração 1 não possui uma conexão com a Internet. Nesse caso, é possível baixar as atualizações usando o Servidor de Administração 2, desde que ele tenha conexão com a Internet e, em seguida, colocar as atualizações em uma pasta local ou de rede para usá-la como fonte de atualização para o Servidor de Administração 1. Caso o Servidor de Administração 2 tenha a versão 13.2 ou anterior, habilite a opção **Baixar atualizações usando o esquema antigo** na tarefa para o Servidor de Administração 1.

Por padrão, esta opção está desativada.

- [Executar verificação de atualizações](#) 

O Servidor de Administração baixa as atualizações da fonte, salva-as num repositório temporário e [executa a tarefa](#) definida no campo **Tarefa de verificação de atualizações**. Se a tarefa for concluída com êxito, as atualizações serão copiadas do repositório temporário para uma pasta compartilhada no Servidor de Administração e distribuídas a todos os dispositivos para os quais o Servidor de Administração atua como a fonte de atualizações (tarefas com o agendamento de **Quando novas atualizações são baixadas no repositório** forem iniciadas). A tarefa de download de atualizações para o repositório é concluída somente após o término da *Tarefa de verificação de atualizações*.

Por padrão, esta opção está desativada.

9. Na janela de propriedades da tarefa, na guia **Agendamento**, crie uma programação 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 Linux.

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 e a hora de início é 18h.

- [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.

- Configurações adicionais da tarefa:

- [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 retardo 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 retardo 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.

- **Parar tarefa se estiver em execução há mais de (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.

10. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Quando o Servidor de Administração executa a tarefa *Baixar atualizações no repositório do Servidor de Administração*, as atualizações de bancos de dados e módulos de software são baixadas da fonte de atualização e armazenadas na pasta compartilhada do Servidor de Administração. Se você criar esta tarefa para um grupo de administração, ela somente será aplicada aos Agentes de Rede incluídos no grupo de administração especificado.

As atualizações são distribuídas aos dispositivos cliente e aos Servidores de Administração secundários da pasta compartilhada do Servidor de Administração.

Visualização de atualizações baixadas

Quando o Servidor de Administração executa a tarefa *Baixar atualizações no repositório do Servidor de Administração*, as atualizações de bancos de dados e módulos de software são baixadas da fonte de atualização e armazenadas na pasta compartilhada do Servidor de Administração. É possível visualizar as atualizações baixadas na seção **ATUALIZAÇÕES PARA OS BANCOS DE DADOS E MÓDULOS DE SOFTWARE DA KASPERSKY**.

Para visualizar a lista de atualizações baixadas,

No menu principal, vá para **OPERAÇÕES** → **APLICATIVOS KASPERSKY** → **ATUALIZAÇÕES PARA OS BANCOS DE DADOS E MÓDULOS DE SOFTWARE DA KASPERSKY**.

Aparece uma lista das atualizações disponíveis.

Verificação das atualizações baixadas

Antes de instalar as atualizações nos dispositivos gerenciados, é possível verificar primeiro as atualizações sobre operabilidade e erros por meio da tarefa de *Verificação de atualizações*. A tarefa de *Verificação de atualizações* é executada automaticamente como parte da tarefa *Baixar atualizações no repositório do Servidor de Administração*. O Servidor de Administração baixa as atualizações da origem, salva-as no armazenamento temporário e executa a tarefa de *Verificação de atualizações*. Caso a tarefa seja concluída com êxito, as atualizações são copiadas do repositório temporário para a pasta compartilhada do Servidor de Administração. Elas são distribuídas à todos os dispositivos cliente para os quais o Servidor de Administração for a fonte de atualizações.

Caso os resultados da tarefa de *Verificação de atualizações* demonstrarem que as atualizações localizadas no repositório temporário estão incorretas ou se a tarefa de *Verificação de atualizações* concluir com erro, as atualizações não serão copiadas para a pasta compartilhada. O Servidor de Administração retém o conjunto anterior de atualizações. Além disso, as tarefas que têm o tipo de agendamento **Quando novas atualizações são baixadas no repositório** não são iniciadas. Essas operações são realizadas no próximo início da tarefa *Baixar atualizações no repositório do Servidor de Administração* se a verificação das novas atualizações for concluída com êxito.

Um conjunto de atualizações é considerado inválido se uma das seguintes condições for atendida em pelo menos um dispositivo de teste:

- Ocorreu um erro na tarefa de atualização.
- O status da proteção em tempo real do aplicativo de segurança foi modificado após a aplicação das atualizações.
- Um objeto infectado foi detectado durante a execução da tarefa de verificação sob demanda.
- Ocorreu um erro de tempo de execução de um aplicativo da Kaspersky.

Caso nenhuma das condições listadas sejam verdadeiras em nenhum dispositivo de teste, o conjunto de atualizações é considerado como válido, e a tarefa de *Verificação de atualizações* será considerada com êxito na conclusão.

Antes de começar a criar a tarefa de *Verificação de atualizações*, execute os pré-requisitos:

1. [Criar um grupo de administração](#) com vários dispositivos de teste. Esse grupo será necessário para verificar as atualizações.

Recomenda-se usar os dispositivos com a proteção mais confiável e com a configuração de aplicativo mais popular na rede. Essa abordagem aumenta a qualidade e a probabilidade de detecção de vírus durante as verificações e minimiza o risco de falsos positivos. Caso sejam detectados vírus nos dispositivos de teste, a tarefa de *Verificação de atualizações* será considerada malsucedida.

2. [Criar as tarefas de atualização e verificação de vírus](#) para um aplicativo compatível com o Kaspersky Security Center, por exemplo, Kaspersky Endpoint Security for Linux. Ao criar as tarefas de atualização e verificação de vírus, especifique o grupo de administração com os dispositivos de teste.

A tarefa de *Verificação de atualizações* executa sequencialmente as tarefas de atualização e verificação de vírus em dispositivos de teste para verificar se todas as atualizações são válidas. Além disso, ao criar a tarefa de *Verificação de atualizações*, será necessário especificar as tarefas de atualização e verificação de vírus.

3. Crie a tarefa [Baixar atualizações no repositório do Servidor de Administração](#).

Para que o Kaspersky Security Center Linux verifique as atualizações baixadas antes de distribuí-las para os dispositivos cliente:

1. No menu principal, vá para **DISPOSITIVOS** → **TAREFAS**.
2. Clique na tarefa **Baixar atualizações no repositório do Servidor de Administração**.

3. Na janela de propriedades do aplicativo que se abre, acesse a guia **Configurações do aplicativo** e, então, habilite a opção **Executar verificação de atualizações**.
4. Caso a tarefa *Verificação de atualizações* exista, clique no botão **Selecionar tarefa**. Na janela aberta, selecione a tarefa de *Verificação de atualizações* no grupo de administração com dispositivos de teste.
5. Caso não tenha criado a tarefa de *Verificação de atualizações* anteriormente, faça o seguinte:

- a. Clique no botão **Nova tarefa**.
- b. No Assistente para Adicionar Tarefa aberto, especifique o nome da tarefa caso queira alterar o nome da predefinição.
- c. Selecione o grupo de administração com os dispositivos de teste criado anteriormente.
- d. Primeiro, selecione a tarefa de atualização de um aplicativo necessário e compatível com o Kaspersky Security Center, em seguida, selecione a tarefa de verificação de vírus.

Depois disso, as seguintes opções aparecem. Recomendamos deixá-las ativadas:

- **Reiniciar o dispositivo após a atualização do banco de dados** 

Depois que os bancos de dados antivírus forem atualizados em um dispositivo, recomendamos reinicializar o dispositivo.

Por padrão, a opção está ativada.

- **Verificar o status de proteção em tempo real após atualização do banco de dados e o reinício do dispositivo** 

Caso esta opção esteja habilitada, a tarefa de *Verificação de atualizações* verifica se as atualizações baixadas para o repositório do Servidor de Administração são válidas e se o nível de proteção diminuiu após a atualização do banco de dados antivírus e a reinicialização do dispositivo.

Por padrão, esta opção está ativada.

- e. Especifique uma conta a partir da qual a tarefa de *Verificação de atualizações* será executada. É possível usar a conta e deixar a opção **Conta padrão** habilitada. Como alternativa, é possível especificar que a tarefa seja executada em outra conta com os direitos de acesso necessários. Para isso, selecione a opção **Especificar conta** e, em seguida, insira as credenciais dessa conta.

6. Clique em **Salvar** para fechar a janela de propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração*.

A verificação de atualizações automática é ativada. Agora, é possível executar a tarefa *Baixar atualizações no repositório do Servidor de Administração*, e ela começará a partir da verificação de atualização.

Criar a tarefa para baixar as atualizações aos repositórios de pontos de distribuição

É possível 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.

Você pode usar esta tarefa, por exemplo, se o tráfego entre o Servidor de Administração e pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.

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 componentes do Kaspersky Security Center
- 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 **DISPOSITIVOS** → **TAREFAS**.
2. Clique no botão **Adicionar**.
O Assistente para Adicionar Tarefas é iniciado. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, 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 etapa **Concluir a criação da tarefa**, caso queira modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída**. 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.

Ao ativar a opção **Não usar servidor proxy** para as fontes de atualização Servidores de atualização da Kaspersky ou Pasta local ou de rede, o ponto de distribuição não usará um servidor proxy para baixar as atualizações, mesmo que a opção **Usar o servidor proxy** do ponto de distribuição das [configurações de política do Agente de Rede](#) esteja habilitada.

- [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](#) ⓘ

A partir da versão 14, o Kaspersky Security Center baixa as atualizações de bancos de dados e os 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 Linux.

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 e a hora de início 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.

- [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 retardo 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 retardo 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.

Adicionando fontes de atualizações para a tarefa Baixar atualizações no repositório do Servidor de Administração

Ao criar ou usar a [tarefa para baixar atualizações para o repositório do Servidor de Administração](#), é possível escolher as seguintes fontes de atualizações:

- Servidores de atualização da Kaspersky
- Servidor de Administração principal

Este recurso é aplicado a tarefas criadas para um Servidor de Administração virtual ou secundário.

- Pasta local ou de rede

Por padrão, são usados os servidores de atualização da Kaspersky, mas também é possível baixar atualizações de uma pasta local ou de rede. Você pode querer usar a pasta se sua rede não tiver acesso à Internet. Nesse caso, é possível baixar manualmente as atualizações dos servidores de atualização da Kaspersky e colocar os arquivos baixados na pasta necessária.

É possível especificar apenas um caminho para uma pasta local ou de rede. Como pasta local, é possível usar apenas uma pasta no Servidor de Administração. Como uma pasta de rede, é possível usar apenas um servidor FTP ou HTTP.

Ao adicionar os servidores de atualização da Kaspersky e a pasta local ou de rede, as atualizações serão baixadas primeiro da pasta. Em caso de erro de download, os servidores de atualização da Kaspersky serão usados.

Caso uma pasta compartilhada que contenha atualizações seja protegida por senha, ative a opção **Especificar conta para acesso à pasta compartilhada da fonte de atualização (se houver)** e insira as credenciais da conta necessárias para o acesso.

Para adicionar as fontes de atualização:

1. Acesse **DISPOSITIVOS** → **TAREFAS**.
2. Clique em **Baixar atualizações no repositório do Servidor de Administração**.
3. Vá para a guia **Configurações do aplicativo**.
4. Na linha **Fontes de atualizações**, clique no botão **Configurar**.
5. Na janela que se abre, clique no botão **Adicionar**.
6. Na lista de fontes de atualização, adicione as fontes necessárias. Ao selecionar a caixa de seleção **Pasta local ou de rede**, especifique um caminho para a pasta.
7. Clique em **OK** e feche a janela de propriedades da fonte de atualização.
8. Na janela da fonte de atualização, clique em **OK**.
9. Clique no botão **Salvar** na janela da tarefa.

Agora as atualizações são baixadas das fontes especificadas para o repositório do Servidor de Administração.

Sobre usar os arquivos diff para atualizar bancos de dados e módulos do software Kaspersky

Quando o Kaspersky Security Center Linux baixa atualizações de servidores de Atualização a partir da Kaspersky, ele otimiza o tráfego usando arquivos diff. Você também pode ativar o uso de arquivos diff pelos dispositivos (Servidores de Administração, pontos de distribuição e dispositivos cliente) que recebem atualizações de outros dispositivos na rede.

Sobre o recurso Baixar arquivos diff

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 poupa 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 no Servidor de Administração ou em um ponto de distribuição, os arquivos diff serão salvos no Servidor de Administração ou ponto de distribuição. Como resultado, os dispositivos que recebem atualizações desse Servidor de Administração ou 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 Servidor de Administração ou 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 Servidor de Administração ou 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.

Ativando o recurso de Baixar arquivos diff: cenário

Fases

1 Como ativar o recurso no Servidor de Administração

Ative o recurso nas configuração de uma tarefa [Baixar atualizações para o repositório do Servidor de Administração](#).

2 Como ativar o recurso para um ponto de distribuição

Ative o recurso em um ponto de distribuição que recebe atualizações por meio de uma tarefa [Baixar atualizações para os repositórios de pontos de distribuição](#).

Em seguida, ative o recurso nas [configurações de política do Agente de Rede](#) para um ponto de distribuição que recebe atualizações do Servidor de Administração.

Em seguida, ative o recurso em um ponto de distribuição que recebe atualizações do Servidor de Administração.

O recurso é ativado nas [configurações de política do Agente de Rede](#) e – se os pontos de distribuição forem atribuídos manualmente e você quiser ignorar as configurações da política – na seção [Pontos de distribuição](#) das propriedades do Servidor de Administração.

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.

Baixar atualizações por pontos de distribuição

O Kaspersky Security Center Linux permite que os pontos de distribuição recebem atualizações do Servidor de Administração, dos servidores da Kaspersky ou de uma pasta local ou de rede.

Para configurar o download da atualização para um ponto de distribuição:

1. Na janela principal do aplicativo, clique no ícone **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 por meio do qual as atualizações serão entregues aos dispositivos clientes no grupo.

4. Na janela de propriedades do ponto de distribuição, selecione a seção **Fonte de atualizações**.

5. Selecione uma origem de atualização para o ponto de distribuição:

- [Fonte de atualizações](#) ⓘ

Selecione uma fonte de atualizações para o ponto de distribuição:

- Para permitir que o ponto de distribuição receba atualizações do Servidor de Administração, selecione **Obter do Servidor de Administração**.
- Para permitir que o ponto de distribuição receba atualizações usando uma tarefa, selecione **Usar tarefa de download de atualizações** e, em seguida, especifique a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*:
 - Se essa tarefa já existir no dispositivo, selecione a tarefa na lista.
 - Se ainda não existir tal tarefa no dispositivo, clique no link **Criar tarefa** para criar uma tarefa. O Assistente para Adicionar Tarefas é iniciado. Siga as instruções do Assistente.

- **Baixar arquivos diff** 

Esta opção ativa o [recurso de download dos arquivos diff](#).

Por padrão, esta opção está ativada.

O ponto de distribuição receberá as atualizações da origem especificada.

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](#) por meio do uso do repositório do Servidor de Administração.

Quando for preciso atualizar bancos de dados e módulos do software em um dispositivo (ou um grupo de dispositivos) que não está conectado ao Servidor de Administração (principal ou secundário), a um ponto de distribuição ou à Internet, você terá de usar fontes alternativas de atualizações, 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 de:

- O Servidor de Administração.

Para ter certeza de que o repositório do Servidor de Administração contém as atualizações necessárias para o aplicativo de segurança instalado em um dispositivo offline, pelo menos um dos dispositivos online gerenciados deve ter o mesmo aplicativo de segurança instalado. Esse aplicativo deve ser configurado para receber as atualizações do repositório do Servidor de administração através da tarefa *Baixar atualizações no repositório do Servidor de Administração*.

- Qualquer dispositivo que tem o mesmo aplicativo de segurança instalado e configurado para receber as atualizações do repositório do Servidor de Administração, um repositório de ponto de distribuição ou diretamente dos servidores de atualização Kaspersky.

Abaixo há um exemplo de configuração de atualizações de bancos de dados e módulos de software copiando-os do repositório do Servidor de Administração.

Para atualizar os bancos de dados e módulos de software da Kaspersky em dispositivos offline:

1. Conecte a unidade removível ao dispositivo onde o Servidor de Administração está instalado.
2. Copie os arquivos de atualizações para a unidade removível.

Por padrão, as atualizações estão localizadas em: \\<nome do servidor>\KLSHARE\Updates.

Como alternativa, você pode configurar o Kaspersky Security Center para copiar regularmente as atualizações para a pasta selecionada. Para isso, use a opção **Copiar as atualizações baixadas em pastas adicionais** nas propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Se você especificar uma pasta localizada em um pen drive ou um disco rígido externo como uma pasta de destino dessa opção, esse dispositivo de armazenamento em massa sempre conterá a versão mais recente das atualizações.

3. Em dispositivos offline, [configure o aplicativo Kaspersky Endpoint Security for Linux](#) 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 Linux.

Depois que a tarefa de atualização for concluída, os bancos de dados e os módulos de software da Kaspersky serão atualizados no dispositivo.

Ajuste de pontos de distribuição e gateways de conexão

Uma estrutura de grupos de administração no Kaspersky Security Center Linux executa as seguintes funções:

- Define o escopo das políticas
Há um modo alternativo para aplicar configurações relevantes nos dispositivos, usando *perfis de política*.
- Define o escopo das tarefas de grupo
Há uma abordagem para definir o escopo das 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, Servidores de Administração virtuais 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 ótima 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.

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.

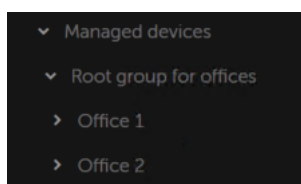
Os seguintes métodos de criar a estrutura de grupos de administração são possíveis:

- 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. Você pode usar a atribuição automática de pontos de distribuição ou atribuí-los manualmente.
- Criar uma estrutura de grupos de administração não levando em consideração a topologia da rede. Nesse caso, é necessário desativar a atribuição automática de pontos de distribuição e, a seguir, 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 atribuí-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.

Calcular o número e a configuração de pontos de distribuição

Quanto mais dispositivos cliente uma rede contiver, mais pontos de distribuição ela exigirá. Recomendamos que você não desative a atribuição automática de pontos de distribuição. Quando a atribuição automática de pontos de distribuição estiver ativada, o Servidor de Administração atribui pontos de distribuição se o número de dispositivos de cliente for bastante grande e define a sua configuração.

Usar pontos de distribuição exclusivamente atribuídos

Se você planejar usar determinados dispositivos específicos como pontos de distribuição (ou seja, servidores exclusivamente atribuídos), você pode optar por não utilizar a atribuição automática de pontos de distribuição. Neste caso, assegure-se de que os dispositivos aos quais você pretende tornar pontos de distribuição tenham 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 estiver desativado (ou não disponível por algum outro motivo), os dispositivos gerenciados no escopo poderão acessar o Servidor de Administração para as atualizações.

Atribuir os pontos de distribuição automaticamente

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center Linux selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos.

Para atribuir os pontos de distribuição automaticamente:

1. Na janela principal do aplicativo, clique no ícone **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. Selecione a opção **Atribuir automaticamente os pontos de distribuição**.

Se a atribuição automática dos dispositivos para agirem como pontos de distribuição estiver ativada, você não pode configurar manualmente os pontos de distribuição nem editar a lista de pontos de distribuição.

4. Clique no botão **Salvar**.

O Servidor de Administração atribui e configura automaticamente os pontos de distribuição.

Atribuir os pontos de distribuição manualmente

O Kaspersky Security Center Linux permite que você atribua dispositivos manualmente para agirem como pontos de distribuição.

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center Linux selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos. No entanto, se você tiver de optar por não atribuir pontos de distribuição automaticamente por algum motivo (por exemplo, se você quiser usar servidores exclusivamente atribuídos), poderá atribuir manualmente os pontos de distribuição após [calcular seu número e configuração](#).

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. Na janela principal do aplicativo, clique no ícone **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. Selecione a opção **Atribuir manualmente os pontos de distribuição**.

4. Clique no botão **Atribuir**.

5. 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.

6. Selecione o grupo de administração que você quer incluir no escopo do ponto de distribuição selecionado.

7. Clique no botão **OK**.

O pontos de distribuição que você adicionou será exibido na lista de pontos de distribuição na seção **Pontos de distribuição**.

8. Selecione o ponto de distribuição recém adicionado na lista para abrir sua janela de propriedades.

9. 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.

- [Número da 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 transmissão múltipla](#) ⓘ

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 de transmissão múltipla](#)

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 Linux atribui automaticamente um endereço IP multicast exclusivo dentro do conjunto especificado.

- [Número da porta multicast IP](#)

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.

- Na seção **Escopo**, especifique os grupos de administração para os quais o ponto de distribuição distribuirá atualizações.
- Na seção **Fonte de atualizações**, você pode selecionar uma fonte de atualizações para o ponto de distribuição:

- [Fonte de atualizações](#) ?

Selecione uma fonte de atualizações para o ponto de distribuição:

- Para permitir que o ponto de distribuição receba atualizações do Servidor de Administração, selecione **Obter do Servidor de Administração**.
- Para permitir que o ponto de distribuição receba atualizações usando uma tarefa, selecione **Usar tarefa de download de atualizações** e, em seguida, especifique a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*:
 - Se essa tarefa já existir no dispositivo, selecione a tarefa na lista.
 - Se ainda não existir tal tarefa no dispositivo, clique no link **Criar tarefa** para criar uma tarefa. O Assistente para Adicionar Tarefas é iniciado. Siga as instruções do Assistente.

- [Baixar arquivos diff](#) ?

Esta opção ativa o [recurso de download dos arquivos diff](#).

Por padrão, esta opção está ativada.

- Configure a pesquisa de intervalos de IP por ponto de distribuição.

- [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 **Ativar sondagem com tecnologia Zeroconf**, 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.

- 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.

10. 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. Acesse **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.

Ativando um servidor push

No Kaspersky Security Center, um ponto de distribuição pode funcionar como um servidor push para os dispositivos gerenciados por meio do protocolo móvel e para os dispositivos gerenciados pelo Agente de Rede. Por exemplo, um servidor push deve ser ativado se você quiser [forçar a sincronização](#) dos dispositivos KasperskyOS com o Servidor de Administração. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Se você tiver vários pontos de distribuição atribuídos ao mesmo grupo de administração, poderá ativar o 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 querer usar pontos de distribuição como servidores push para garantir que haja 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 um ponto de distribuição seja usado como servidor push, não será necessário usar a opção **Não desconecte do Servidor de Administração** nos dispositivos gerenciados ou enviar pacotes para a porta UDP do agente de rede.

Um servidor push suporta a carga de até 50.000 conexões simultâneas.

Para ativar o servidor push em um ponto de distribuição:

1. Clique no ícone **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 no qual deseja ativar o servidor push.
A janela Propriedades do ponto de distribuição é aberta.
4. Na seção **Geral**, selecione a opção **Executar servidor push**.
5. No campo **Porta do servidor push**, digite o número da porta. Você pode especificar o número de qualquer porta livre.
6. No campo **Endereço para hosts remotos**, especifique o endereço IP ou o nome do dispositivo do ponto de distribuição.
7. Clique no botão **OK**.

O servidor push é ativado no ponto de distribuição selecionado.

Gerenciar aplicativos de terceiros em dispositivos cliente

Esta seção descreve os recursos do Kaspersky Security Center Linux relacionados ao gerenciamento de aplicativos de terceiros sendo executados nos dispositivos cliente.

Cenário: Gerenciamento de Aplicativos

Você pode gerenciar a inicialização de aplicativos nos dispositivos do usuário. Você pode permitir ou bloquear a execução de aplicativos em dispositivos gerenciados. Essa funcionalidade é realizada pelo componente Controle de Aplicativos.

O componente do Controle de Aplicativos para o Kaspersky Endpoint Security 11.2 for Linux e versões posteriores.

Pré-requisitos

- O Kaspersky Security Center Linux está implementado em sua organização.
- A Política do Kaspersky Endpoint Security for Linux foi criada e está ativa.

Fases

O cenário de uso do Controle de Aplicativos prossegue em fases:

1 Formar e visualizar a lista de arquivos executáveis em dispositivos cliente

Esta fase 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 armazenados em dispositivos cliente](#)

2 Criar categorias de aplicativo para os aplicativos usados na sua organização

Analise a lista de 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 usuários usarem conjuntos diferentes de aplicativos em seu trabalho, uma categoria de aplicativo poderá ser criada para cada grupo de usuários.

Instruções: [Criando uma categoria de aplicativos com conteúdo adicionado manualmente](#)

3 Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Linux

Configure o componente Controle de Aplicativos na política do Kaspersky Endpoint Security for Linux usando as categorias de aplicativos criadas na fase anterior.

4 Verificar a configuração do Controle de Aplicativos

Certifique-se de ter feito o seguinte:

- Categorias de aplicativos criadas.
- Configurado o Controle de Aplicativos usando as categorias de aplicativos.

Resultados

Quando o cenário estiver concluído, a inicialização dos aplicativos nos dispositivos gerenciados será controlada. Os usuários podem iniciar apenas aqueles aplicativos permitidos na sua organização e não podem iniciar aplicativos proibidos na sua organização.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte a [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 do Controle de Aplicativos para o Kaspersky Endpoint Security 11.2 for Linux e versões posteriores.

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. Este modo 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 Linux, você pode criar apenas [categorias 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.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte a [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 armazenados em dispositivos gerenciados. Para o inventário de arquivos executáveis, você deve criar uma tarefa de inventário.

O Kaspersky Endpoint Security 11.2 for Linux e versões posteriores fornecem o recurso de inventário de arquivos executáveis.

Para criar uma tarefa de inventário para arquivos executáveis em dispositivos cliente:

1. Acesse **DISPOSITIVOS** → **TAREFAS**.

A lista de tarefas é exibida.

2. Clique no botão **Adicionar**.

O [Assistente para Novas Tarefas](#) inicia. Siga as etapas do Assistente.

3. Na página **Nova tarefa**, na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Linux.

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 ser concluída, 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 a Ajuda online do Kaspersky Endpoint Security for Linux.

Após a tarefa **Inventário** ser executada, a lista de arquivos executáveis armazenados 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:

Na lista suspensa **OPERAÇÕES** → **APLICATIVOS DE TERCEIROS**, selecione **ARQUIVOS EXECUTÁVEIS**.

A página exibe a lista de arquivos executáveis armazenados nos dispositivos cliente.

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. Na lista suspensa **OPERAÇÕES** → **APLICATIVOS DE TERCEIROS**, selecione **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 do Assistente **Selecionar método de criação de categoria**, 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 de condição para incluir arquivos na criação da categoria.

5. Na página **Critérios da condição**, selecione um tipo de regra para a criação de categoria na lista:

- [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 instalada em dispositivos na sua rede, é preciso selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center Linux de arquivos nessa 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. Kaspersky Endpoint Security for Linux é compatível com cálculo da SHA-256.

Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center Linux de arquivos na categoria:

- Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem Kaspersky Endpoint Security for Linux, marque a caixa de seleção **SHA-256**.
- Marque a caixa de seleção **Hash MD5** somente se você usar o Kaspersky Endpoint Security for Windows. O Kaspersky Endpoint Security for Linux não oferece suporte à função de 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.

- [Da pasta arquivada](#) 

Se esta opção estiver selecionada, você pode especificar uma pasta de arquivamento e selecionar a condição desejada para usar para adicionar aplicativos à categoria de usuário. A pasta de arquivamento é desempacotada e as condições selecionadas são aplicadas aos arquivos na pasta. Como condição, você pode selecionar uma das seguintes categorias:

- **Hash do arquivo**

Você seleciona que função hash (MD5 ou SHA-256) deseja usar para calcular os valores de hash. Os aplicativos que têm o mesmo valor de hash que os arquivos na pasta de arquivamento são adicionados à categoria de aplicativos do usuário.

Selecione a função de hash MD5 somente se você usar o Kaspersky Endpoint Security for Windows. O Kaspersky Endpoint Security for Linux não oferece suporte à função de hash MD5.

- **Metadados**

Você seleciona que metadados deseja usar como critérios. Os arquivos executáveis que contenham os mesmos metadados serão adicionados à categoria de aplicativos do usuário.

- **Certificado**

Você seleciona quais propriedades de certificado (assunto do certificado, impressão digital ou emissor) deseja usar como critérios. Arquivos executáveis que tenham sido assinados com os certificados contendo as mesmas propriedades serão adicionados à categoria de 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 de condição exclusivo para excluir arquivos da categoria que está sendo criada.
7. Na página **Crítérios 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 a [Ajuda on-line do Kaspersky Endpoint Security for Linux](#).

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,

Na guia **OPERAÇÕES**, na lista suspensa **APLICATIVOS DE TERCEIROS**, selecione **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.

Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos

Após configurar o Controle de Aplicativos nas políticas do Kaspersky Endpoint Security for Linux, 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 de bloqueio da inicialização do aplicativo para o administrador** (evento *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. Acesse **MONITORAMENTO E RELATÓRIOS** → **SELEÇÕES DE EVENTOS**.

A lista de seleções de evento 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 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)** ⓘ

Selecione esta opção somente se você usar o Kaspersky Endpoint Security for Windows. O Kaspersky Endpoint Security for Linux não oferece suporte a uma função de hash MD5.

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.

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 a [Ajuda on-line do Kaspersky Endpoint Security for Linux](#) ⓘ.

Monitoramento e relatórios

Esta seção descreve os recursos de monitoramento e emissão de relatórios no Kaspersky Security Center Linux. Esses recursos fornecem uma visão geral da infraestrutura, dos status de proteção e das estatísticas.

Após a implementação do Kaspersky Security Center Linux ou durante a operação, você pode configurar os recursos de monitoramento e emissão de relatórios de forma a melhor atender 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 Linux.

Pré-requisitos

Após ter implementado o Kaspersky Security Center Linux na rede de uma organização, você poderá iniciar o seu monitoramento e gerar relatórios sobre o seu funcionamento.

O monitoramento e relatórios em na rede de uma organização prossegue em estágios:

1 Configurar a alternância dos status do dispositivo

Conheça as configurações para os status do dispositivo dependendo de condições específicas. [Modificando essas configurações](#), você pode alterar o número de eventos com os níveis de importância *Crítico* ou *Advertência*. 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 como proceder:

[Configure a notificação \(por e-mail, SMS ou executando um arquivo executável\) de eventos em dispositivos cliente](#)

3 Execução das ações recomendadas para as notificações Crítico e Advertência

Instruções de como proceder:

[Execute as ações recomendadas para a rede da sua organização](#)

4 Análise do status de segurança da rede da sua organização

Instruções de como proceder:

- [Revise o widget Status de proteção](#)
- [Gere e revise o Relatório do status de proteção](#)
- [Gere e revise o Relatório de erros](#)

5 Localize dispositivos cliente que não estão protegidos

Instruções de como proceder:

- [Revise o widget Novos dispositivos](#)
- [Gere e revise o Relatório de implementação da proteção](#)

6 Verificação da proteção de dispositivos cliente

Instruções de como proceder:

- [Gere e revise os relatórios das categorias Status de proteção e Estatísticas de ameaças](#)
- [Inicie e analise a seleção de eventos de Crítico](#)

7 Avaliação e limitação da carga de eventos no banco de dados

As informações sobre eventos que ocorrem 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 de como proceder:

- [Limitação do número máximo de eventos](#)

8 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 revise 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 14 Web Console fornece os seguintes tipos de monitoramento e relatórios na rede da sua organização:

- Painel
- Relatórios
- Seleções de eventos
- Notificações

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 definidas pelos usuários baseado nas configurações disponíveis para configuração na interface do Kaspersky Security Center 14 Web Console.

Notificações

As Notificações alertam sobre os eventos e ajudam a agilizar as respostas a estes eventos executando ações recomendadas ou ações que você considera apropriadas.

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 14 Web 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 14 Web Console tem um conjunto padrão de widgets para as seguintes categorias:

- **Status de 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).

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 (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 seção **USUÁRIOS E FUNÇÕES** → **USUÁRIOS**. Pode ser um servidor primário 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**.
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, 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 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 14 Web Console, na seção **MONITORAMENTO E RELATÓRIOS**, clicando em **RELATÓRIOS**.

Por padrão, os relatórios contêm informações dos últimos 30 dias.

O Kaspersky Security Center Linux tem um conjunto padrão de relatórios para as seguintes categorias:

- **Status de 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**.
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.
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.
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.

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.

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, conseqüentemente, você não poderá exibir o relatório.

Por padrão, esta opção está ativada. O valor predefinido é de 1.000.

- **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 predefinido é de 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 predefinido é de 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. Clique no botão **Fechar** (X) para fechar a janela **Edição de relatório <Nome do relatório>**.

O modelo de relatório atualizado aparece na lista de modelos de relatório.

Exportar um relatório para um arquivo

Você pode exportar um relatório para um arquivo XML, HTML ou PDF.

Para exportar um relatório para um arquivo:

1. Acesse **MONITORAMENTO E RELATÓRIOS** → **RELATÓRIOS**.
2. Marque a caixa de seleção ao lado do relatório que deseja exportar para um arquivo.
3. Clique no botão **Exportar relatório**.
4. Na janela exibida, altere o nome do arquivo de relatório no campo **Nome**. Por padrão, o nome do arquivo coincide com o nome do modelo de relatório selecionado.
5. Selecione o tipo de arquivo de relatório: XML, HTML ou PDF.

A ferramenta wkhtmltopdf é necessária para converter um relatório em PDF. Ao selecionar a opção PDF, o Servidor de Administração verifica se a ferramenta wkhtmltopdf está instalada no dispositivo. Se a ferramenta não estiver instalada, o aplicativo exibirá uma mensagem sobre a necessidade de instalar a ferramenta no dispositivo do Servidor de Administração. Instale a ferramenta manualmente e prossiga para a próxima etapa.

6. Clique no botão **Exportar relatório**.

O relatório no formato selecionado será baixado para o seu dispositivo (para a pasta padrão do seu dispositivo), ou uma janela padrão **Salvar como** será exibida no navegador para permitir que você salve o arquivo onde quiser.

O relatório é salvo no arquivo.

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.

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. Acesse **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.

A ferramenta wkhtmltopdf é necessária para converter um relatório em PDF. Ao selecionar a opção PDF, o Servidor de Administração verifica se a ferramenta wkhtmltopdf está instalada no dispositivo. Se a ferramenta não estiver instalada, o aplicativo exibirá uma mensagem sobre a necessidade de instalar a ferramenta no dispositivo do Servidor de Administração. Instale a ferramenta manualmente e prossiga para a próxima etapa.
 - c. Se os relatórios precisarem ser enviados por e-mail, em conjunto com as configurações de notificação por e-mail.
 - d. Se os relatórios precisarem ser salvos em uma pasta, se os relatórios anteriormente salvos nessa pasta precisarem ser sobrescrito e se uma conta específica precisar ser usada para acessar a pasta (para uma pasta compartilhada).
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 Linux e sobre como gerenciar o bloqueio de eventos frequentes.

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 definidas pelos usuários baseado nas configurações disponíveis para configuração na interface do Kaspersky Security Center 14 Web Console.

As seleções de eventos estão disponíveis no Kaspersky Security Center 14 Web 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 Linux 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](#).

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 Linux 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 seleções de eventos.

Editar uma seleção de eventos

Para editar uma seleção de eventos:

1. No menu principal, vá para **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 evento

Para visualizar a seleção de eventos:

1. No menu principal, vá para **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.

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.

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, vá para **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.

Configuração do termo de armazenamento de um evento

O Kaspersky Security Center Linux 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. Pode ser necessário armazenar alguns eventos por um período maior ou menor do que o especificado pelos valores padrão. Você pode alterar as configurações padrão do período de armazenamento de um evento.

Se não desejar em armazenar alguns eventos no banco de dados do Servidor de Administração, poderá desativar a respectiva configuração na política do Servidor de Administração e na política do aplicativo Kaspersky, ou nas propriedades do Servidor de Administração (apenas para eventos do Servidor de Administração). Isso reduzirá o número de tipos de evento no banco de dados.

Quanto mais longo o prazo de armazenamento de um evento, mais rápido o banco de dados atingirá sua capacidade máxima. No entanto, um prazo de armazenamento mais longo de um evento permite executar tarefas de monitoramento e relatório por um período de tempo maior.

Para definir o prazo de armazenamento de um evento no banco de dados do Servidor de Administração:

1. Selecione **DISPOSITIVOS** → **POLÍTICAS E PERFIS**.

2. Execute uma das seguintes ações:

- Para configurar o termo de armazenamento dos eventos do Agente de Rede ou de um aplicativo Kaspersky gerenciado, clique no nome da política correspondente.

A janela de página da política será aberta.

- Para configurar os eventos do Servidor de Administração, na parte superior da tela, clique no ícone de **Configurações** (⚙️) ao lado do nome do Servidor de Administração necessário.

Se você possui uma política para o Servidor de Administração, pode clicar no nome dessa política.

A página de propriedades do Servidor de Administração (ou a página de propriedades da política do Servidor de Administração) é aberta.

3. Selecione a guia **Configuração de eventos**.

Uma lista de tipos de evento relacionados à seção **Crítico** é exibida.

4. Selecione a seção **Falha funcional**, **Advertência** ou **Informações**.

5. Na lista de tipos de eventos no painel direito, clique no link do evento cujo prazo de armazenamento deseja alterar.

Na seção **Registro de eventos** da janela, a opção **Armazenar no banco de dados do Servidor de Administração por (dias)** é ativada.

6. Na caixa de edição abaixo desse botão de alternar, insira o número de dias para armazenar o evento.

7. Caso não deseje armazenar um evento no banco de dados do Servidor de Administração, desative a opção **Armazenar no banco de dados do Servidor de Administração por (dias)**.

Se você configurar eventos do Servidor de Administração na janela de propriedades do Servidor de Administração e se as configurações do evento estiverem bloqueadas na política do Servidor de Administração do Kaspersky Security Center Linux, não será possível redefinir o valor do período de armazenamento para um evento.

8. Clique em **OK**.

A janela de propriedades da política é fechada.

A partir de agora, quando o Servidor de Administração receber e armazenar os eventos do tipo selecionado, eles terão o prazo de armazenamento alterado. O Servidor de Administração não altera o prazo de armazenamento de eventos recebidos anteriormente.

Tipos de eventos

Cada componente do Kaspersky Security Center Linux tem o seu próprio conjunto de tipos de evento. Esta seção lista os tipos de eventos que ocorrem no Servidor de Administração e no Agente de Rede do Kaspersky Security Center Linux. Os tipos de eventos que ocorrem nos aplicativos Kaspersky não são listados nesta seção.

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 Linux 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 vistas públicas fornecidas no banco de dados do Kaspersky Security Center Linux e quando os eventos são exportados para um sistema SIEM.
- **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. Se você configurou para salvar os eventos no log de eventos do sistema operacional, poderá encontrá-los nesse local.

Você pode alterar o prazo de armazenamento para eventos: [Definir o prazo de armazenamento para um evento](#)

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 mostra os eventos do Servidor de Administração do Kaspersky Security Center Linux com o nível de importância **Crítico**.

Eventos críticos do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenar padrão
O limite da licença foi excedido	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Uma vez por dia o Kaspersky Security Center Linux verifica se a restrição de licenciamento foi excedida.	180 dias

			<p>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.</p> <p>Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos.</p> <p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • 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). <p>O Kaspersky Security Center Linux determina as regras para gerar eventos quando uma restrição de licenciamento for excedida.</p>	
O dispositivo está sem	4111	KLSRV_HOST_OUT_CONTROL	Eventos deste tipo ocorrem se um	180 dias

gerenciamento			<p>dispositivo gerenciado está visível na rede, mas não se conectou ao Servidor de Administração por um período de tempo específico.</p> <p>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.</p>	
O status do dispositivo é Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	<p>Eventos deste tipo ocorrem quando um dispositivo gerenciado é atribuído com o status <i>Crítico</i>. Você pode configurar as condições sob as quais o status do dispositivo é alterado para <i>Crítico</i>.</p>	180 dias
O arquivo de chave foi adicionado à lista de bloqueio	4124	KLSRV_LICENSE_BLACKLISTED	<p>Eventos deste tipo ocorrem quando a Kaspersky tiver adicionado o código de ativação ou arquivo de chave usado por você à lista de proibição.</p> <p>Entre em contato com o Suporte Técnico para obter mais detalhes.</p>	180 dias
A licença expira em breve	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	<p>Eventos desse tipo ocorrem quando a data de expiração da licença comercial está se aproximando.</p>	180 dias

			<p>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.</p> <p>Quando a licença comercial expirar, o Kaspersky Security Center Linux fornecerá apenas a funcionalidade básica.</p> <p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • 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	Eventos deste tipo ocorrem quando o certificado do Servidor de Administração para	180 dias

			<p>Gerenciamento de Dispositivos Móveis expira.</p> <p>Você precisa atualizar o certificado expirado.</p> <p>Você pode configurar atualizações automáticas de certificados selecionando a caixa de seleção Reemitir o certificado automaticamente se possível nas configurações de emissão de certificado.</p>
--	--	--	---

Eventos de falha funcional do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração do Kaspersky Security Center Linux com o nível de importância **Falha funcional**.

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
Erro do tempo de execução	4125	KLSRV_RUNTIME_ERROR	<p>Eventos deste tipo ocorrem devido a problemas desconhecidos.</p> <p>Mais frequentemente estes são problemas de DBMS, problemas de rede e outros problemas de software e hardware.</p> <p>Os detalhes do evento podem ser encontrados na descrição do evento.</p>	180 dias
O limite de instalações foi excedido para um dos grupos de aplicativos licenciados	4126	KLSRV_INVLICPROD_EXCEEDED	<p>O Servidor de Administração gera periodicamente eventos deste tipo (a cada hora). Eventos deste tipo ocorrem se no Kaspersky Security Center Linux você gerencia chaves de licença de aplicativos</p>	180 dias

			<p>de terceiros e o número de instalações excedeu o limite definido pela chave de licença do aplicativo de terceiro.</p> <p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • Examine a lista de dispositivos gerenciados. Exclua o aplicativo de terceiro dos dispositivos nos quais o aplicativo não está em uso. • Use uma licença de terceiro para mais dispositivos. <p>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.</p>	
Falha ao copiar as atualizações para a pasta especificada	4123	KLSRV_UPD_REPL_FAIL	<p>Eventos deste tipo ocorrem quando as atualizações do software são copiadas para uma pasta adicional compartilhada.</p> <p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • Verifique se a conta de usuário que está sendo empregada para obter o acesso às pastas tem permissão de gravação. • Verifique se um nome de usuário 	180 dias

			<p>e/ou senha para a pasta foi alterado.</p> <ul style="list-style-type: none"> • Verifique a conexão com a internet, já que isso pode ser a causa do evento. Siga as instruções para atualizar bancos de dados e módulos do software. 	
Nenhum espaço livre em disco	4107	KLSRV_DISK_FULL	<p>Eventos deste tipo ocorrem quando o disco rígido do dispositivo onde o Servidor de Administração está instalado fica sem espaço.</p> <p>Libere espaço em disco no dispositivo.</p>	180 dias
A pasta compartilhada não está disponível	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	<p>Eventos deste tipo ocorrem se a pasta compartilhada do Servidor de Administração não estiver disponível.</p> <p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • Verifique se o Servidor de Administração (onde a pasta compartilhada está localizada) está ativado e disponível. • Verifique se um nome de usuário e/ou senha para a pasta foi/está alterado. • Verifique a conexão à rede. 	180 dias
O banco de dados do Servidor de Administração está indisponível	4109	KLSRV_DATABASE_UNAVAILABLE	<p>Eventos deste tipo ocorrem se o banco de dados do Servidor de Administração s tornar indisponível.</p>	180 dias

			<p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • Verifique se o servidor remoto que tem o SQL Server instalado está disponível. • Visualize os registros do DBMS para descobrir o motivo da indisponibilidade de banco de dados do Servidor de Administração. Por exemplo, devido a uma manutenção preventiva de um servidor remoto com o SQL Server instalado possa estar indisponível. 	
<p>Espaço insuficiente no banco de dados do Servidor de Administração</p>	4110	KLSRV_DATABASE_FULL	<p>Eventos deste tipo ocorrem quando não houver nenhum espaço livre no banco de dados do Servidor de Administração.</p> <p>O Servidor de Administração não funciona quando seu banco de dados alcançou sua capacidade e quando o registro no banco de dados não for possível.</p> <p>A seguir estão as causas deste evento, dependendo do DBMS que você usa, e as respostas apropriadas ao evento:</p> <ul style="list-style-type: none"> • Você usa o SQL Server Express Edition DBMS: <ul style="list-style-type: none"> • Na documentação do SQL Server Express, verifique o limite de 	180 dias

tamanho do banco de dados para a versão que estiver usando. Provavelmente, o banco de dados de seu Servidor de Administração excedeu o limite de tamanho.

- [Limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração.](#)

- No banco de dados do Servidor de Administração, há muitos eventos enviados pelo componente Controle de Aplicativos. Você pode alterar as configurações da política do Kaspersky Endpoint Security for Linux relacionadas ao armazenamento de eventos do Controle de Aplicativos no banco de dados do Servidor de Administração.

- Você usa um DBMS diferente do SQL Server Express Edition:

- [Não limite o número de eventos a serem 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.](#)

Revise as informações na seleção do DBMS.

Eventos de aviso do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração do Kaspersky Security Center Linux com o nível de importância **Advertência**.

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 armazenamento padrão
O limite da licença foi excedido	4098	KLSRV_EV_LICENSE_CHECK_100_110	<p>Uma vez por dia o Kaspersky Security Center Linux verifica se a restrição de licenciamento foi excedida.</p> <p>Eventos deste tipo ocorrem quando o Servidor de Administração detecta 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.</p>	90 dias

			<p>Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos.</p> <p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • 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). <p>O Kaspersky Security Center Linux determina as regras para gerar eventos quando uma restrição de licenciamento for excedida.</p>	
O dispositivo permaneceu inativo na rede por muito tempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	<p>Eventos desse tipo ocorrem quando um dispositivo gerenciado fica em inatividade por algum tempo.</p> <p>Na maioria das vezes, isso acontece quando um dispositivo gerenciado é desativado.</p> <p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • Remova manualmente o dispositivo da lista de dispositivos gerenciados. 	90 dias

			<p>Especifique o intervalo de tempo após o qual o evento O dispositivo permaneceu inativo na rede por muito tempo é criado usando o Kaspersky Security Center 14 Web Console.</p> <ul style="list-style-type: none"> Especifique o intervalo de tempo após o qual o dispositivo é removido automaticamente do grupo usando o Kaspersky Security Center 14 Web Console. 	
Conflito de nomes de dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	<p>Eventos desse tipo ocorrem quando o Servidor de Administração considera dois ou mais dispositivos gerenciados como um único dispositivo.</p> <p>Na maioria das vezes, isso acontece quando um disco rígido clonado foi usado para implantação de software em dispositivos gerenciados, sem alterar o Agente de Rede para o modo de clonagem de disco dedicado em um dispositivo de referência.</p> <p>Para evitar este problema, altere o Agente de Rede para o modo de clonagem de disco em um dispositivo de referência antes de clonar o disco rígido desse dispositivo.</p>	90 dias
O status do	4114	KLSRV_HOST_STATUS_WARNING	Eventos deste tipo	90 dias

dispositivo é Advertência			ocorrem quando à um dispositivo gerenciado for atribuído o status de <i>Aviso</i> . Você pode configurar as condições sob as quais o status do dispositivo é alterado para <i>Aviso</i> .	
O limite de instalações está prestes a ser excedido para um dos grupos de aplicativos licenciados	4127	KLSRV_INVLICPROD_FILLED	<p>Eventos deste tipo ocorrem quando o número de instalações de aplicativos de terceiros incluídos em um grupo de aplicativos licenciados atinge 90% do valor máximo permitido especificado nas propriedades da chave de licença.</p> <p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • Se o aplicativo de terceiros não estiver em uso em alguns dos dispositivos gerenciados, exclua o aplicativo desses dispositivos. • Se você espera que o número de instalações do aplicativo de terceiros ultrapasse o máximo permitido em um futuro próximo, considere obter uma licença de terceiros para um número maior de dispositivos com antecedência. 	90 dias

			Você pode gerenciar chaves de licença de aplicativos de terceiros usando a funcionalidade de grupos de aplicativos licenciados.	
O certificado foi solicitado	4133	KLSRV_CERTIFICATE_REQUESTED	<p>Eventos deste tipo ocorrem quando um certificado para Gerenciamento de Dispositivos Móveis não é reemitido automaticamente.</p> <p>Seguem abaixo as possíveis causas e as respostas apropriadas para o evento:</p> <ul style="list-style-type: none"> • A reemissão automática foi iniciada para um certificado para o qual a opção Reemitir o certificado automaticamente se possível está desativada. Isso pode ser devido a um erro ocorrido durante a criação do certificado. Pode ser necessária a reemissão manual do certificado. • Se você usar uma integração com uma infraestrutura de chave pública, a causa pode ser a ausência de um atributo SAM-Account-Name na conta usada para integração com PKI e para emissão do certificado. Revise as propriedades da conta. 	90 dias
O certificado foi removido	4134	KLSRV_CERTIFICATE_REMOVED	Eventos deste tipo ocorrem quando um	90 dias

			<p>administrador remove qualquer tipo de certificado (Geral, Correio, VPN) para Gerenciamento de Dispositivos Móveis.</p> <p>Depois de remover um certificado, os dispositivos móveis conectados por meio deste certificado não conseguirão se conectar ao Servidor de Administração.</p> <p>Este evento pode ser útil ao investigar falhas associadas ao gerenciamento de dispositivos móveis.</p>	
O certificado de APNs expirou	4135	KLSRV_APN_CERTIFICATE_EXPIRED	<p>Eventos deste tipo ocorrem quando um certificado de APNs expira.</p> <p>Você precisa renovar manualmente o certificado de APNs e instalá-lo em um servidor de MDM do iOS.</p>	Não armazenado
O certificado de APNs expira em breve	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	<p>Eventos deste tipo ocorrem quando faltam menos de 14 dias para a expiração do certificado de APNs.</p> <p>Quando o certificado de APNs expirar, você precisará renová-lo manualmente e instalá-lo em um servidor de MDM do iOS.</p> <p>Recomendamos que você agende a renovação do certificado de APNs antes da data de expiração.</p>	Não armazenado
Falha ao enviar a mensagem FCM para o dispositivo móvel	4138	KLSRV_GCM_DEVICE_ERROR	<p>Eventos desse tipo ocorrem quando o Gerenciamento de Dispositivos Móveis está configurado para usar o Google Firebase Cloud Messaging (FCM)</p>	90 dias

			<p>para se conectar a dispositivos móveis gerenciados com um sistema operacional Android e o Servidor FCM não consegue processar algumas das solicitações recebidas do Servidor de Administração. Isso significa que alguns dos dispositivos móveis gerenciados não receberão uma notificação push.</p> <p>Leia o código HTTP nos detalhes da descrição do evento e resposta de acordo. Para obter mais informações sobre os códigos HTTP recebidos do Servidor de FCM e erros relacionados, consulte a documentação do serviço Google Firebase (em especial, o capítulo "Códigos de resposta de erro de mensagens downstream").</p>	
Ocorreu um erro de HTTP ao enviar a mensagem FCM para o servidor FCM	4139	KLSRV_GCM_HTTP_ERROR	<p>Eventos desse tipo ocorrem quando o Gerenciamento de Dispositivos Móveis está configurado para usar o Google Firebase Cloud Messaging (FCM) para se conectar a dispositivos móveis gerenciados com sistema operacional Android e o Servidor FCM responde à solicitação do Servidor de Administração com um código HTTP diferente de 200 (OK).</p>	90 dias

			<p>Seguem abaixo as possíveis causas e as respostas apropriadas para o evento:</p> <ul style="list-style-type: none"> • Problemas no lado do servidor FCM. Leia o código HTTP nos detalhes da descrição do evento e responda de acordo. Para obter mais informações sobre os códigos HTTP recebidos do Servidor de FCM e erros relacionados, consulte a documentação do serviço Google Firebase (em especial, o capítulo "Códigos de resposta de erro de mensagens downstream"). • Problemas no lado do servidor proxy (se estiver usando servidor proxy). Leia o código HTTP nos detalhes do evento e responda de acordo. 	
Falha ao enviar a mensagem FCM para o servidor FCM	4140	KLSRV_GCM_GENERAL_ERROR	<p>Eventos deste tipo ocorrem devido a erros inesperados no Servidor de Administração ao trabalhar com o protocolo HTTP do Google Firebase Cloud Messaging.</p> <p>Leia os detalhes na descrição do evento e responda de acordo.</p>	90 dias

			Se você não conseguir solucionar o problema sozinho, é recomendável entrar em contato com o Suporte Técnico da Kaspersky.	
Pouco espaço livre no disco rígido	4105	KLSRV_NO_SPACE_ON_VOLUMES	<p>Eventos deste tipo ocorrem quando o disco rígido do dispositivo onde o Servidor de Administração está instalado fica praticamente sem espaço livre.</p> <p>Libere espaço em disco no dispositivo.</p>	90 dias
Resta pouco espaço livre no banco de dados do Servidor de Administração	4106	KLSRV_NO_SPACE_IN_DATABASE	<p>Eventos deste tipo ocorrem se o espaço no banco de dados do Servidor de Administração for muito limitado. Se você não remediar a situação, em breve o banco de dados do Servidor de Administração alcançará sua capacidade e o Servidor de Administração não funcionará.</p> <p>A seguir estão as causas deste evento, dependendo do DBMS que estiver usando, e as respostas apropriadas ao evento.</p> <p>Você usa o SQL Server Express Edition DBMS:</p> <ul style="list-style-type: none"> • Na documentação do SQL Server Express, verifique o limite de tamanho do banco de dados para a versão que estiver usando. Provavelmente, o banco de dados de seu Servidor de Administração 	90 dias

está por alcançar seu limite de tamanho.

- [Limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração.](#)
- No banco de dados do Servidor de Administração, há muitos eventos enviados pelo componente Controle de Aplicativos. Você pode alterar as configurações da política do Kaspersky Endpoint Security for Linux relacionadas ao armazenamento de eventos do Controle de Aplicativos no banco de dados do Servidor de Administração. Você usa um DBMS diferente do SQL Server Express Edition:
- [Não limite o número de eventos a serem 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](#)

Revise as informações na seleção do DBMS.

			<p>está por alcançar seu limite de tamanho.</p> <ul style="list-style-type: none">• <u>Limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração.</u>• No banco de dados do Servidor de Administração, há muitos eventos enviados pelo componente Controle de Aplicativos. Você pode alterar as configurações da política do Kaspersky Endpoint Security for Linux relacionadas ao armazenamento de eventos do Controle de Aplicativos no banco de dados do Servidor de Administração. Você usa um DBMS diferente do SQL Server Express Edition:• <u>Não limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração</u>• <u>Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração</u> <p>Revise as informações na seleção do DBMS.</p>	
A conexão	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Eventos deste tipo	90 dias

com o Servidor de Administração secundário foi interrompida			<p>ocorrem quando uma conexão com o Servidor de Administração secundário é interrompida.</p> <p>Leia o Log de eventos Kaspersky no dispositivo onde o Servidor de Administração primário está instalado e responda de acordo.</p>	
A conexão com o Servidor de Administração principal foi interrompida	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	<p>Eventos deste tipo ocorrem quando uma conexão com o Servidor de Administração primário é interrompida.</p> <p>Leia o Log de eventos Kaspersky no dispositivo onde o Servidor de Administração primário está instalado e responda de acordo.</p>	90 dias
Novas atualizações para os módulos de software da Kaspersky foram registradas	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	<p>Eventos deste tipo ocorrem quando o Servidor de Administração registra novas atualizações para o software Kaspersky instalado em dispositivos gerenciados que requerem aprovação para instalação.</p> <p>Aprove ou recuse as atualizações usando o Kaspersky Security Center Web Console.</p>	90 dias
O limite de eventos no banco de dados foi excedido. A exclusão dos eventos foi iniciada	4145	KLSRV_EVP_DB_TRUNCATING	<p>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.</p>	Não armazenado

			<p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Você pode responder ao evento nas seguintes maneiras:</p> <ul style="list-style-type: none"> • Alterar o número máximo permitido de eventos a ser 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 	Não armazenad

Eventos informativos do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração do Kaspersky Security Center Linux com o nível de importância **Informações**.

Eventos informativos do Servidor de Administração

Nome de exibição do tipo de	ID de	Tipo de evento	Prazo de
-----------------------------	-------	----------------	----------

evento	tipo de evento		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 adicionado automaticamente ao grupo	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	4144	KLSRV_UPD_BASES_UPDATED	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: a conexão com o Servidor de Administração foi encerrada	4151	KLAUD_EV_SERVERDISCONNECT	30 dias
Auditoria: as propriedades do objeto foram modificadas	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 dias
Auditoria: as permissões do usuário foram modificadas	4153	KLAUD_EV_OBJECTACLMODIFIED	30 dias

Eventos do Agente de Rede

Esta seção contém informações sobre os eventos relativos ao Agente de Rede.

Eventos de aviso do Agente de Rede

A tabela abaixo mostra os eventos do Agente de Rede do Kaspersky Security Center Linux que têm o nível de gravidade **Advertência**.

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
Ocorreu um incidente	549	GNRL_EV_APP_INCIDENT_OCCURED	30 dias

Eventos informativos do Agente de Rede

A tabela abaixo mostra os eventos do Agente de Rede do Kaspersky Security Center Linux que têm o nível de gravidade **Informações**.

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
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
Novo dispositivo adicionado	7708	KLNAG_EV_DEVICE_ARRIVAL	30 dias
Dispositivo removido	7709	KLNAG_EV_DEVICE_REMOVE	30 dias
Novo dispositivo detectado	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dias
O dispositivo foi autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 dias

Bloqueio de eventos frequentes

Esta seção fornece informações sobre como gerenciar e remover o bloqueio de eventos frequentes.

Sobre o bloqueio de eventos frequentes

Um aplicativo gerenciado, por exemplo, Kaspersky Endpoint Security for Linux, instalado em um ou vários dispositivos gerenciados, pode enviar muitos eventos do mesmo tipo ao Servidor de Administração. Receber eventos frequentes pode sobrecarregar o banco de dados do Servidor de Administração e sobrepor-se a outros eventos. O Servidor de Administração começa a bloquear os eventos mais frequentes quando o número de todos os eventos recebidos excede o [limite especificado para o banco de dados](#).

O Servidor de Administração bloqueia o recebimento automático de eventos frequentes. Você não pode bloquear os eventos frequentes ou escolher quais eventos bloquear.

Caso queira saber se um evento está bloqueado, é possível visualizar a lista de notificações ou visualizar se o evento está presente na seção **Bloqueando eventos frequentes** das propriedades do servidor de administração. Se o evento estiver bloqueado, você pode fazer o seguinte:

- Se deseja evitar a substituição do banco de dados, pode [continuar bloqueando](#) o recebimento desse tipo de evento.
- Se deseja, por exemplo, localizar o motivo do envio de eventos frequentes ao Servidor de Administração, pode [desbloquear](#) os eventos frequentes e continuar recebendo os eventos deste tipo de qualquer maneira.
- Se quiser continuar recebendo os eventos frequentes até que sejam bloqueados novamente, pode [remover o bloqueio](#) dos eventos frequentes.

Gerenciando o bloqueio de eventos frequentes

O Servidor de Administração bloqueia o recebimento automático de eventos frequentes, mas você pode desbloquear e continuar a recebê-los. Você também pode bloquear o recebimento de eventos frequentes que desbloqueou anteriormente.

Para gerenciar o bloqueio de eventos frequentes:

1. Na janela principal do aplicativo, clique no ícone **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 **Bloquear eventos frequentes**.

3. Na seção **Bloquear eventos frequentes**:

- Se deseja desbloquear o recebimento de eventos frequentes:
 - a. Selecione os eventos frequentes que deseja desbloquear e clique no botão **Excluir**.
 - b. Clique no botão **Salvar**.
- Se deseja bloquear o recebimento de eventos frequentes:
 - a. Selecione os eventos frequentes que deseja bloquear e clique no botão **Bloquear**.

b. Clique no botão **Salvar**.

O Servidor de Administração recebe os eventos frequentes desbloqueados e não recebe os eventos frequentes bloqueados.

Removendo o bloqueio de eventos frequentes

Você pode remover o bloqueio de eventos frequentes e começar a recebê-los até que o Servidor de Administração os bloqueie novamente.

Para remover o bloqueio de eventos frequentes:

1. Na janela principal do aplicativo, clique no ícone **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 **Bloquear eventos frequentes**.

3. Na seção **Bloquear eventos frequentes**, selecione os tipos de eventos frequentes os quais deseja remover o bloqueio.

4. Clique no botão **Remover do bloqueio**.

O evento frequente é removido da lista de eventos frequentes. O Servidor de Administração receberá eventos deste tipo.

Processamento e armazenamento do evento no Servidor de Administração

As informações sobre eventos durante a operação do aplicativo gerenciado e de dispositivos gerenciados são salvas no banco de dados do Servidor de Administração. Cada evento é atribuído a um determinado tipo e nível de gravidade (*Evento crítico*, *Falha funcional*, *Advertência* ou *Informativo*). Dependendo das condições sob as quais um evento ocorreu, o aplicativo pode atribuir diferentes níveis de gravidade aos eventos do mesmo tipo.

Você pode visualizar os tipos e níveis de gravidade atribuídos aos eventos na seção **Configuração do evento** da janela Propriedades do Servidor de Administração. Na seção **Configuração do evento**, você também poderá configurar o processamento de cada evento pelo Servidor de Administração:

- O registro de eventos no Servidor de Administração e nos registros de evento do sistema operacional em um dispositivo cliente e no Servidor de Administração.
- Método usado para notificar o administrador sobre um evento (por exemplo, um SMS ou mensagem de e-mail).

Na seção **Repositório de eventos** da janela Propriedades do Servidor de Administração, você pode editar as configurações de armazenamento do evento no banco de dados do Servidor de Administração ao limitar o número de registros de evento ou o tempo de armazenamento do registro. Quando você especifica o número máximo de eventos, o aplicativo calcula um volume aproximado do espaço de armazenamento necessário para o número especificado. Você pode usar esse cálculo aproximado para avaliar se você tem espaço livre suficiente no disco para evitar sobrecarga do banco de dados. A capacidade padrão do banco de dados do Servidor de Administração é de 400.000 eventos. A capacidade máxima recomendada do banco de dados é de 45 milhões de eventos.

Se o número de eventos no banco de dados atingir o valor máximo especificado pelo administrador, o aplicativo exclui os eventos mais antigos e regravava com os novos eventos. Quando o Servidor de Administração exclui eventos antigos, não pode salvar novos eventos no banco de dados. Durante esse período de tempo, as informações sobre eventos rejeitados são gravadas no Log de Eventos Kaspersky. Os novos eventos são colocados em fila e salvos no banco de dados depois que a operação de exclusão é concluída.

Notificações e status do dispositivo

Esta seção contém informações sobre como visualizar notificações, configurar a entrega de notificações, usar o status do dispositivo e habilitar a alteração de status do dispositivo.

Usar as notificações

As Notificações alertam sobre os eventos e ajudam a agilizar as respostas a estes eventos executando ações recomendadas ou ações que você considera apropriadas.

Dependendo do método de notificação selecionado, os seguintes tipos de notificações estão disponíveis:

- Notificações na tela
- Notificações por SMS
- Notificações por e-mail
- Notificações por arquivo executável ou script

Notificações na tela

As notificações na tela alertam para eventos agrupados por níveis de importância (*Crítico*, *Aviso* e *Informativo*).

A notificação na tela pode ter um de dois status:

- *Revisado*. Significa que você executou a ação recomendada para a notificação ou atribuiu esse status da notificação manualmente.
- *Não Revisado*. Significa que você não executou a ação recomendada para a notificação ou não atribuiu esse status da notificação manualmente.

Por padrão, a lista de notificações inclui notificações no status *Não Revisado*.

Você pode monitorar a rede da sua organização [visualizando notificações na tela](#) e dando resposta a elas em tempo real.

Notificações por e-mail, por SMS e por arquivo executável ou um script

O Kaspersky Security Center Linux 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 notificações por e-mail, SMS ou executando um arquivo executável ou um script](#).

Para receber notificações por e-mail ou SMS, você pode decidir a sua resposta para um evento. Essa resposta deve ser a mais apropriada para a rede da sua organização. Executando um arquivo executável ou um script, você predefine uma resposta para um evento. Você também pode considerar a execução de um arquivo executável ou um script como uma resposta primária para um evento. Após a execução do arquivo executável, você pode tomar outras medidas para responder ao evento.

Visualização de notificações na tela

Você pode visualizar notificações na tela de três maneiras:

- Na seção **MONITORAMENTO E RELATÓRIOS** → **NOTIFICAÇÕES**. Aqui, você pode exibir notificações relacionadas a categorias predefinidas.
- Em uma janela separada que pode ser aberta, não importa qual seção está sendo usada no momento. Neste caso, você pode marcar notificações como revisadas.
- No widget **Notificações por nível de gravidade selecionado** na seção **MONITORAMENTO E RELATÓRIOS** → **PAINEL**. No widget, você pode exibir apenas notificações de eventos que estão nos níveis de importância *Crítico e Aviso*.

Você pode realizar ações, por exemplo, responder a um evento.

Para visualizar notificações de categorias predefinidas:

1. No menu principal, vá para **MONITORAMENTO E RELATÓRIOS** → **NOTIFICAÇÕES**.

A categoria **Todas as notificações** é selecionada no painel esquerdo, e no painel direito todas as notificações são exibidas.

2. No painel esquerdo, selecione uma das categorias:

- **Implementação**
- **Dispositivos**
- **Proteção**
- **Atualizações** (esta inclui notificações sobre aplicativos Kaspersky disponíveis para download e notificações sobre atualizações de banco de dados de antivírus que foram baixadas)
- **Prevenção de Exploit**
- **Servidor de Administração** (esta inclui eventos relacionados apenas ao Servidor de Administração)
- **Links úteis** (esta inclui links para recursos da Kaspersky, por exemplo, Suporte Técnico da Kaspersky, fórum da Kaspersky, página de renovação de licença ou a Enciclopédia de TI da Kaspersky)
- **Notícias da Kaspersky** (esta inclui informações sobre versões de aplicativos Kaspersky)

Uma lista de notificações da categoria selecionada é exibida. A lista contém o seguinte:

- Ícone relacionado ao tópico da notificação: implementação (🔧), proteção (🛡️), atualizações (🔄), gerenciamento de dispositivo (📱), Prevenção de Exploits (🔒), Servidor de Administração (🏢).

- Nível de importância da notificação. As notificações dos seguintes níveis de importância são exibidas: **Notificações críticas** (🔴), **Notificações de advertência** (⚠️), **Notificações de informação**. As notificações na lista são agrupadas por níveis de importância.
- **Notificação**. Contém uma descrição da notificação.
- **Ação**. Contém um link para uma ação rápida que recomendamos que você execute. Por exemplo, clicando neste link, você pode prosseguir para o repositório e instalar aplicativos de segurança em dispositivos ou visualizar uma lista de dispositivos ou uma lista de eventos. Depois que executar a ação recomendada para a notificação, essa notificação será atribuída ao status *Revisado*.
- **Status registrado**. Contém o número de dias ou horas que se passaram a partir do momento em que a notificação foi registrada no Servidor de Administração.

Para exibir notificações na tela em uma janela separada pelo nível de importância:

1. No canto superior direito do Kaspersky Security Center 14 Web Console, clique no ícone de **Indicador** (🔔).

Se o ícone **Sinalizador** tiver um ponto vermelho, isso significa que há notificações que não foram revisadas.

Uma janela é exibida listando as notificações. Por padrão, a guia **Todas as notificações** está selecionada, e as notificações estão agrupadas pelo nível de importância: *Crítico*, *Aviso* e *Informativo*.

2. Selecione a guia **Sistema**.

A lista de notificações de níveis de importância *Crítico* (🔴) e *Advertência* (⚠️) é exibida. A lista de notificações inclui o seguinte:

- Marcador de cores. As notificações críticas estão marcadas em vermelho. As notificações de aviso estão marcadas em amarelo.
- Ícone que indica o tópico da notificação: implementação (🔧), proteção (🛡️), atualizações (🔄), gerenciamento de dispositivo (📱), Prevenção de Exploits (🛑), Servidor de Administração (🏢).
- Descrição da notificação.
- Ícone **Sinalizador**. O ícone de **Sinalizador** ficará cinza se as notificações tiverem recebido o status *Não Revisado*. Quando você seleciona o ícone de **Sinalizador** cinza e atribui o status *Revisado* a uma notificação, a cor do ícone muda para branca.
- Link para a ação recomendada. Quando você executa a ação recomendada depois de clicar no link, a notificação ganha o status *Revisado*.
- O número de dias que se passaram desde a data quando a notificação foi registrada no Servidor de Administração.

3. Selecione a guia **Mais**.

A lista de notificações de nível de importância *Informativo* é exibida.

A organização da lista é a mesma da lista na guia **Sistema** (veja a descrição acima). A única diferença é a ausência de um marcador de cores.

Você pode filtrar notificações pelo intervalo de datas quando elas tiverem sido registradas no Servidor de Administração. Use a caixa de seleção **Mostrar filtro** para gerenciar o filtro.

Para exibir notificações na tela no widget:

1. Na seção **PAINEL**, selecione **Adicionar ou restaurar widget da Web**.

2. Na janela exibida, clique na categoria **Outro**, selecione o widget **Notificações por nível de gravidade selecionado** e clique em [Adicionar](#).

O widget agora aparece na guia **PAINEL**. Por padrão, as notificações do nível de importância *Crítico* são exibidas no widget.

Você pode clicar no botão **Configurações** no widget e [alterar as configurações de widget](#) para exibir notificações do nível de importância *Aviso*. Ou você pode adicionar outro widget: **Notificações por nível de gravidade selecionado**, com um nível de importância *Aviso*.

A lista de notificações no widget é limitada pelo seu tamanho e inclui duas notificações. Essas duas notificações estão relacionadas aos eventos mais recentes.

A lista de notificações no widget inclui o seguinte:

- Ícone relacionado ao tópico da notificação: implementação (🔧), proteção (🛡️), atualizações (🔄), gerenciamento de dispositivo (📱), Prevenção de Exploits (🛡️), Servidor de Administração (🖥️).
- Descrição da notificação com um link para a ação recomendada. Quando você executa a ação recomendada depois de clicar no link, a notificação ganha o status *Revisado*.
- O número de dias ou o número de horas que se passaram desde a data quando a notificação foi registrada no Servidor de Administração.
- Link para outras notificações. Clicando nesse link, você é transferido para a visualização de notificações na seção **NOTIFICAÇÕES** em **MONITORAMENTO E RELATÓRIOS**.

Sobre os status do dispositivo

O Kaspersky Security Center Linux 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 Linux leva em consideração o sinalizador de visibilidade do dispositivo na rede (consulte a tabela abaixo). Se o Kaspersky Security Center Linux 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.	<ul style="list-style-type: none">• O botão de alternar é ativado.

		<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Parado. • Pausada. • Executando.
A verificação de vírus não é executada há muito tempo	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas a tarefa de verificação de vírus não foi executada 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.	<ul style="list-style-type: none"> • O botão de alternar é desativado. • O botão de alternar é ativado.
A licença expirou	O dispositivo está visível na rede, mas a licença expirou.	<ul style="list-style-type: none"> • O botão de alternar é desativado. • O botão de alternar é ativado.
A licença	O dispositivo está visível na rede, mas a licença expirará no dispositivo	Mais de 0 dias.

expira em breve	em tempo menor que o número especificado de dias.	
Incidentes não processados detectados	Alguns incidentes não processados foram encontrados no dispositivo. Os incidentes podem ser criados automaticamente, através de aplicativos da Kaspersky gerenciados instalados no dispositivo cliente, ou manualmente pelo administrador.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 <i>Crítico</i> ou <i>Advertência</i> é alterado para o status <i>OK</i> 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.	<ul style="list-style-type: none"> • 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.	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.	<ul style="list-style-type: none"> • O botão de alternar é desativado. • O botão de alternar é ativado.

O Kaspersky Security Center Linux permite definir a troca 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*.

Se você atualizar o Kaspersky Security Center Linux da versão anterior, os valores da condição **Os bancos de dados estão desatualizados** para atribuir o status *Crítico* ou *Aviso* não mudam.

Quando o Kaspersky Security Center Linux 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 **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 **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 sobre eventos que ocorrem no Kaspersky Security Center Linux. Dependendo do método de notificação selecionado, os seguintes tipos de notificações estão disponíveis:

- E-mail — sempre que ocorre um evento, Kaspersky Security Center Linux envia uma notificação para os endereços de e-mail especificados.
- SMS — sempre que ocorre um evento, Kaspersky Security Center Linux envia uma notificação para os números de telefone especificados.
- Arquivo executável — sempre que ocorre um evento, o arquivo executável é executado no Servidor de Administração.

Para configurar a entrega de notificação de eventos que ocorrem no Kaspersky Security Center Linux:

1. Na parte superior da tela, 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, selecione a guia do método de notificação desejado:

- [E-mail](#) ⓘ

A guia **E-mail** permite-lhe configurar a notificação do evento por e-mail.

No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Se você ativar a opção **Usar consulta de DNS MX**, pode usar vários registros MX dos endereços IP para o mesmo nome DNS do servidor SMTP. O mesmo nome DNS pode ter vários registros de MX com valores diferentes de prioridade de recebimento de mensagens de e-mail. O Servidor de Administração tenta enviar notificações por e-mail ao servidor SMTP em ordem crescente de prioridade dos registros MX.

Se você ativar **Usar consulta de DNS MX** e não ativar o uso de configurações TLS, recomendamos que use as configurações DNSSEC em seu dispositivo de servidor como uma medida adicional de proteção para o envio de notificações por e-mail.

Se você ativar a opção **Usar a autenticação ESMTP**, pode especificar as configurações de autenticação ESMTP nos campos **Nome do usuário** e **Senha**. Por padrão, a opção estiver desativada, e as configurações da autenticação ESMTP não estão disponíveis.

Você pode especificar as configurações de TLS de conexão com um servidor SMTP:

- **Não usar TLS**

Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.

- **Usar TLS se compatível com servidor SMTP**

Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.

- **Sempre usar TLS e verificar a validade do certificado do servidor**

Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

Se você selecionar o valor **Sempre usar TLS e verificar a validade do certificado do servidor**, pode especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar certificados para uma conexão TLS clicando no link **Especificar certificados**:

- Procurar por um arquivo de certificado do servidor SMTP:

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center Linux verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável. O Kaspersky Security Center Linux não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

- Procurar um arquivo de certificado de cliente:

Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer autoridade de certificação confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

- Certificado X-509:

Você deve especificar um arquivo com o certificado e um arquivo com a chave privada. Ambos os arquivos não dependem um do outro e a ordem de carregamento dos arquivos não é significativa. Quando os dois arquivos são carregados, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

- Contêiner pkcs12:

Você deve carregar um único arquivo que contenha o certificado e sua chave privada. Quando o arquivo for carregado, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

Clicar no botão **Enviar mensagem de teste** permite verificar se você configurou as notificações apropriadamente: o aplicativo envia uma notificação de teste aos endereços de e-mail que você especificou.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula.

No campo **Assunto**, especifique o assunto do e-mail. Você pode deixar este campo vazio.

Na lista suspensa **Modelo de assunto**, selecione o modelo do seu assunto. Uma variável determinada pelo modelo selecionado é colocada automaticamente no campo **Assunto**. Você pode criar um assunto de e-mail selecionando vários modelos de assunto.

No campo **Endereço de e-mail do remetente: se essa configuração não for especificada, o endereço do destinatário será usado em vez disso**. **Aviso: não é recomendável usar um endereço de e-mail fictício**, especifique o endereço de e-mail do remetente. Se você deixar este campo vazio, por padrão, o endereço do destinatário é usado. Não é recomendável usar endereços de e-mail fictícios.

O campo **Mensagem de notificação** contém o texto padrão com informações sobre o evento que o aplicativo envia quando ocorrer um evento. Este texto inclui parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio. Você pode editar o texto da mensagem adicionando outros [parâmetros substitutos](#) com detalhes mais relevantes sobre o evento.

Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clicar no link **Configurar limite numérico de notificações** permite-lhe especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.

- [SMS](#) 

A guia **SMS** permite-lhe configurar a transmissão de notificações por SMS de vários eventos para um telefone celular. As mensagens SMS é enviadas por meio de um gateway de correio.

No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Caso a opção **Usar a autenticação ESMTP** seja ativada, será possível especificar as configurações de autenticação ESMTP nos campos **Nome do usuário** e **Senha**. Por padrão, a opção estiver desativada, e as configurações da autenticação ESMTP não estão disponíveis.

Você pode especificar as configurações de TLS de conexão com um servidor SMTP:

- **Não usar TLS**

Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.

- **Usar TLS se compatível com servidor SMTP**

Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.

- **Sempre usar TLS e verificar a validade do certificado do servidor**

Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

Se você selecionar o valor **Sempre usar TLS e verificar a validade do certificado do servidor**, pode especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar o arquivo de certificado do servidor SMTP clicando no link **Especificar certificados**. Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center Linux verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável. O Kaspersky Security Center Linux não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula. As notificações serão entregues aos números de telefone associados aos endereços de e-mail especificados.

No campo **Assunto**, especifique o assunto do e-mail.

Na lista suspensa **Modelo de assunto**, selecione o modelo do seu assunto. Uma variável segundo o modelo selecionado é inserida no campo **Assunto**. Você pode criar um assunto de e-mail selecionando vários modelos de assunto.

No campo **Endereço de e-mail do remetente**: se essa configuração não for especificada, o endereço do destinatário será usado em vez disso. **Aviso: não é recomendável usar um endereço de e-mail fictício**, especifique o endereço de e-mail do remetente. Se você deixar este campo vazio, por padrão, o endereço do destinatário é usado. Não é recomendável usar endereços de e-mail fictícios.

No campo **Números de telefone dos destinatários de mensagens SMS**, especifique os números de celular dos destinatários da notificação de SMS.

O campo **Mensagem de notificação**, especifique um texto padrão com informações sobre o evento que o aplicativo envia quando ocorrer um evento. Este texto pode incluir [parâmetros substitutos](#), como o nome do evento, nome do dispositivo e nome do domínio.

Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clique em **Enviar mensagem de teste** para verificar se você configurou as notificações adequadamente: o aplicativo envia uma notificação de teste ao destinatário especificado.

Clique no link **Configurar limite numérico de notificações** para especificar a quantidade máxima de notificações que o aplicativo pode enviar ao longo do intervalo de tempo especificado.

- [Arquivo executável a ser executado](#) 

Se este método de notificação estiver selecionado, no campo de entrada, você pode especificar o aplicativo que será iniciado quando ocorre um evento.

No campo **O arquivo executável que será executado no Servidor de Administração quando um evento ocorrer**, especifique a pasta e o nome do arquivo a ser executado. Antes de especificar o arquivo, [prepare-o e especifique os espaços reservados](#) que definem os detalhes do evento a serem enviados na mensagem de notificação. A pasta e o arquivo especificados devem estar localizados no Servidor de Administração.

Clicar no link **Configurar limite numérico de notificações** permite-lhe especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.

3. Na guia, defina as configurações de notificação.

4. Clique no botão **OK** para fechar a janela Propriedades do Servidor de Administração.

As configurações de entrega de notificação salvas são aplicadas a todos os eventos que ocorrem no Kaspersky Security Center Linux.

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.

Testar as notificações

Para verificar se as notificações de eventos foram enviadas, o aplicativo usa a notificação da detecção de vírus de teste EICAR em dispositivos cliente.

Para verificar o envio das notificações de eventos:

1. Interrompa a tarefa de proteção em tempo real do sistema de arquivos no dispositivo cliente e copie o vírus de teste EICAR para o dispositivo cliente. Em seguida, ative novamente a proteção em tempo real no sistema de

arquivos.

2. Execute uma tarefa de verificação para dispositivos cliente em um grupo de administração ou para dispositivos específicos, inclusive um com o vírus EICAR.

Se a tarefa de verificação estiver configurada corretamente, o vírus de teste será detectado. Se as notificações estiverem configuradas corretamente, você será notificado que um vírus foi detectado.

Para abrir um registro da detecção de vírus de teste:

1. No menu principal, vá para **MONITORAMENTO E RELATÓRIOS** → **SELEÇÕES DE EVENTOS**.
2. Clique no nome da seleção **Eventos recentes**.

A notificação sobre o vírus de teste é exibida na janela que se abre.

O vírus de teste de EICAR não contém nenhum código que possa danificar seu dispositivo. No entanto, a maioria dos aplicativos de segurança de fabricantes identifica esse arquivo como um vírus. Você pode fazer download do vírus de teste no [site oficial da EICAR](#).

Notificações de evento exibidas executando um arquivo executável

O Kaspersky Security Center Linux pode notificar o administrador sobre eventos em dispositivos clientes processando um arquivo executável. O arquivo executável deve conter outro arquivo executável com marcadores de posição do evento a enviar para o administrador.

Marcadores de posição para descrever um evento

Marcador de posição	Descrição do marcador de posição
%SEVERITY%	Nível de importância do evento
%COMPUTER%	Nome do dispositivo onde ocorreu o evento
%DOMAIN%	Domínio
%EVENT%	Evento
%DESCR%	Descrição de evento
%RISE_TIME%	Hora de criação
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nome da tarefa
%KL_PRODUCT%	Agente de Rede do Kaspersky Security Center Linux
%KL_VERSION%	Número da versão do Agente de Rede
%HOST_IP%	Endereço IP
%HOST_CONN_IP%	Endereço IP de conexão

Exemplo:

As notificações de eventos são enviadas através de um arquivo executável (como script1.bat) dentro do qual outro arquivo executável (como script2.bat) com o marcador de posição %COMPUTER% é executado. Quando um evento ocorrer, o arquivo script1.bat é executado no dispositivo do administrador, o qual, por sua vez, executa o arquivo script2.bat com o marcador de posição %COMPUTER%. O administrador recebe o nome do dispositivo no qual o evento ocorreu.

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 e sobre aplicativos gerenciados instalados nos dispositivos gerenciados. O Kaspersky Security Center atualiza periodicamente as informações da seção, removendo informações antigas e adicionando novas.

O Kaspersky Security Center mostra apenas os anúncios da 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.

O Servidor de Administração deve ter uma conexão com a internet para receber os informativos da Kaspersky.

Os informativos têm como objetivo manter os aplicativos 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. Por padrão, os anúncios da Kaspersky estão ativados. Se não deseja receber informações sobre novidades da Kaspersky, [pode desativar este recurso](#).

Para mostrar a você as informações que correspondem à sua configuração de proteção de rede, o Kaspersky Security Center 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 de Licença do Usuário Final](#) aceito por você ao instalar o Servidor de Administração do Kaspersky Security Center.

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 14 Web 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.

Você pode especificar as [configurações de Novidades Kaspersky](#), incluindo as categorias de informações que deseja receber e onde exibir o rótulo de notificação. Se não deseja receber informações sobre novidades, você pode [desativar este recurso](#).

Especificando configurações para receber as Novidades Kaspersky

Na seção [Novidades Kaspersky](#), você pode especificar as configurações de Novidades Kaspersky, incluindo as categorias de notícias que deseja receber e onde exibir o rótulo de notificação.

Para desativar o recebimento das Novidades Kaspersky:

1. No menu principal, vá para **MONITORAMENTO E RELATÓRIOS** → **NOVIDADES KASPERSKY**.
2. Clique no link **Configurações**.
A janela de configurações de Novidades Kaspersky é aberta.
3. Especificar as seguintes configurações:
 - Selecione o nível de importância para as novidades que você deseja ver. As novidades sobre outras categorias não serão exibidas.
 - Selecione onde você deseja que o rótulo de notificação seja exibido. O rótulo pode ser exibido em todas as seções do console ou na seção **MONITORAMENTO E RELATÓRIOS** e suas subseções.
4. Clique no botão **OK**.
As configurações da seção Novidades Kaspersky estão especificadas.

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 e sobre aplicativos gerenciados instalados nos dispositivos gerenciados. Se não deseja receber informações de novidades sobre a Kaspersky, pode desativar este recurso.

Para desativar o recebimento de novidades sobre a Kaspersky:

1. Na janela principal do aplicativo, clique no ícone **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 **Novidades Kaspersky**.
3. Use o botão de alternância para mudar para a posição **Novidades relacionadas à segurança** estão desativadas.
4. Clique no botão **Salvar**.
O recebimento de novidades sobre a Kaspersky está desativado.

Exportação de 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

O Kaspersky Security Center Linux permite configurar a exportação de eventos para sistemas SIEM por um dos seguintes métodos: exportar para qualquer sistema SIEM que use o formato Syslog ou exportar eventos para sistemas SIEM diretamente do banco de dados do Kaspersky Security Center. Ao concluir este cenário, o Servidor de Administração envia eventos para um sistema SIEM automaticamente.

Pré-requisitos

Antes de iniciar a exportação de configuração de eventos no Kaspersky Security Center Linux:

- [Saiba mais sobre os métodos de exportação de eventos](#).
- Certifique-se de que tem conhecimento dos [os valores das configurações do sistema](#).

Você pode executar as etapas deste cenário em qualquer ordem.

O processo de exportação de eventos para um sistema SIEM consiste nos seguintes passos:

- **Configurando o sistema SIEM para receber eventos do Kaspersky Security Center Linux**

Instruções: [Configurando a exportação de eventos em um sistema SIEM](#)

- **Selecionando os eventos que deseja exportar para o sistema SIEM**

Marcar quais eventos deseja exportar para o sistema SIEM. Primeiro, [marque os eventos gerais](#) que ocorrem em todos os aplicativos gerenciados da Kaspersky. Depois disso, é possível [marcar os eventos para aplicativos gerenciados específicos da Kaspersky](#).

- **Configurando a exportação de eventos para o sistema SIEM**

É possível exportar eventos usando um dos seguintes métodos:

- [Usando TCP/IP, UDP ou TLS via protocolos TCP](#)
- Usando a exportação de eventos diretamente do [banco de dados do Kaspersky Security Center](#) (um conjunto de visualizações públicas é fornecido no banco de dados do Kaspersky Security Center. Você pode encontrar a descrição destas visualizações públicas no documento [klakdb.chm](#)).

Resultados

Após configurar a exportação de eventos para um 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 Linux, 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 Linux.

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 Linux e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center Linux e nas configurações do receptor do seu sistema SIEM.

- [Protocolo](#)

Protocolo usado para transferir mensagens do Kaspersky Security Center Linux ao seu sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center Linux e nas configurações do receptor do seu sistema SIEM.

Sobre eventos no Kaspersky Security Center Linux

O Kaspersky Security Center Linux 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. Você pode 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 Linux, 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 visualizar 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, também é possível visualizar a lista de eventos nas propriedades do Servidor de Administração.

Os eventos podem ser gerados pelos seguintes aplicativos:

- Componentes do Kaspersky Security Center Linux:
 - [Servidor de Administração](#)
 - [Agente de Rede](#)

- Aplicativos Kaspersky gerenciados

Para obter detalhes sobre os eventos gerados pelos aplicativos gerenciados pela Kaspersky, consulte a documentação do aplicativo correspondente.

Nível de importância por eventos

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 Linux. 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.

Sobre a exportação de evento

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 Linux para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center Linux) 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 Linux. Não importa que lado você configura primeiro. É possível configurar a transmissão de eventos no Kaspersky Security Center Linux 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 Linux. 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.

Sobre a configuração de exportação de eventos em um sistema SIEM

O processo de exportar eventos do Kaspersky Security Center Linux para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center Linux) e um receptor do evento (sistema SIEM). Você deve configurar a exportação de eventos no seu sistema SIEM e no Kaspersky Security Center Linux.

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 Linux, configure o receptor no seu sistema SIEM. Em geral, as seguintes configurações devem ser especificadas no sistema SIEM:

- **Protocolo para exportar**

Um protocolo de transferência de mensagens, UDP, TCP ou TLS, sobre TCP. Este protocolo deve ser o mesmo protocolo que você especificou no Kaspersky Security Center Linux.

- **Porta**

Especifique o número da porta para se conectar ao Kaspersky Security Center Linux. A porta deve ser a mesma [especificada no Kaspersky Security Center Linux durante a configuração com um sistema SIEM](#).

- **Formato de dados**

Especifique o formato Syslog.

Dependendo do sistema SIEM usado, você pode ter que especificar algumas configurações adicionais de receptor.

A figura abaixo mostra tela de configuração de receptor no ArcSight.

The screenshot shows the 'Edit Receiver' configuration page in the ArcSight Logger interface. The page has a navigation bar at the top with 'hp ArcSight Logger' and tabs for 'Summary', 'Analyze', 'Dashboards', 'Configuration', and 'System Admin'. Below the navigation bar, the title 'Edit Receiver' is displayed. A note states: 'If a source type that you need does not exist in the Source Type dropdown list below, go to the [Source Types](#) page to add it.' The configuration fields are: 'Name' (text input: tcp cef), 'IP/Host' (dropdown: All), 'Port' (text input: 616), 'Encoding' (dropdown: UTF-8), 'Source Type' (dropdown: CEF), and 'Enable' (checkbox: checked). At the bottom, there are 'Save' and 'Cancel' buttons.

Configuração do receptor no ArcSight

Analizador 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; eles 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 Linux para que eles possam ser armazenados no banco de dados do sistema SIEM.

Cada sistema SIEM tem um conjunto de analisadores de mensagem padrão. A Kaspersky também fornece analisadores de mensagem para alguns sistemas SIEM, por exemplo, para QRadar e ArcSight. Você pode baixar destes analisadores de mensagem dos sites dos sistemas SIEM correspondentes. Ao configurar o receptor, você pode selecionar para usar um dos analisadores de mensagem padrão ou um analisador de mensagem da Kaspersky.

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 selecionar 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 deseja 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 **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 **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:

- Clique no ícone **Configurações** (⚙️) ao lado do nome do Servidor de Administração necessário.
- No menu principal, vá para **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 usado para exportar os eventos do Kaspersky Security Center Linux aos sistemas externos.

No Kaspersky Security Center Linux, 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 Linux é configurado para que ele envie eventos ao sistema SIEM. O Kaspersky Security Center Linux 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 Linux 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 Linux.

Para configurar a exportação para sistemas SIEM no Kaspersky Security Center 14 Web Console:

1. Na lista suspensa **Configurações do console**, selecione **Integração**.

A janela **Configurações do console** se abre.

2. Selecione a guia **Integração**.

3. Na guia **Integração**, selecione a seção **SIEM**.

4. Clique no link **Configurações**.

A seção **Exportar as configurações** é aberta.

5. 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 Linux e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center Linux e nas configurações do receptor do seu sistema SIEM.

- [Protocolo](#) 

Selecione o protocolo a ser usado para transferir mensagens para o sistema SIEM. Você pode selecionar o TCP/IP, UDP ou TLS sobre protocolo TCP.

Especifique as seguintes configurações de TLS se selecionar o protocolo TLS sobre TCP:

- **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 para o Kaspersky Security Center Linux. O Kaspersky Security Center Linux verifica se o certificado do servidor do sistema SIEM também é assinado por CAs confiáveis ou não.

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. Para adicionar uma impressão digital SHA-1, insira-a no campo **Impressões digital** 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. Assim, você usará um certificado autoassinado emitido pelo Kaspersky Security Center. 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 Linux não pode se conectar ao servidor do sistema SIEM se o nome de domínio do servidor do sistema SIEM 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 Linux valida 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.

- **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 certificado no campo **Arquivo com certificado** e um arquivo com 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. Como resultado, o Kaspersky Security Center Linux armazena o certificado autoassinado gerado e você pode passar a parte pública do certificado ou a impressão digital SHA1 para o sistema SIEM.

6. 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**.
7. Altere a opção para a posição **Exportar automaticamente eventos para o banco de dados do sistema SIEM ATIVADO**.
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.

Exportando eventos diretamente do banco de dados

Você pode recuperar eventos diretamente do banco de dados do Kaspersky Security Center Linux sem ter necessidade de usar a interface Kaspersky Security Center Linux. Você pode consultar as vistas públicas diretamente e recuperar os dados de evento ou criar as suas próprias vistas com base em vistas públicas existentes e endereçá-las para receber os dados de que precisa.

Vistas públicas

Para a sua conveniência, um conjunto de vistas públicas é fornecido no banco de dados do Kaspersky Security Center Linux. Você pode encontrar a descrição destas vistas públicas no documento [klakdb.chm](#).

A vista pública `v_akpub_ev_event` contém um conjunto de campos que representa os parâmetros de evento no banco de dados. No documento `klakdb.chm` você também pode encontrar informações sobre vistas públicas que correspondem a outras entidades do Kaspersky Security Center Linux, por exemplo, dispositivos, aplicativos ou usuários. Você pode usar estas informações nas suas consultas.

Esta seção contém instruções para criar uma consulta SQL por meio do utilitário `ksql2` e um exemplo de consulta.

Para criar consultas SQL ou vistas do banco de dados, você também pode usar qualquer outro programa para trabalhar com bancos de dados. As informações sobre como exibir os parâmetros para conectar-se ao banco de dados do Kaspersky Security Center Linux, como o nome da instância e o nome do banco de dados, são fornecidas na seção correspondente.

Criar uma consulta SQL usando o utilitário `ksql2`

Esta seção descreve como baixar e usar o utilitário klsq2, e como criar uma consulta SQL usando este utilitário. Quando você cria uma consulta SQL por meio do utilitário klsq2, não precisa fornecer o nome do banco de dados e os parâmetros de acesso, porque a consulta endereça diretamente as vistas públicas do Kaspersky Security Center Linux.

Para baixar e usar o utilitário klsq2:

1. Baixe o [utilitário klsq2](#) do site da Kaspersky.
2. Copie e extraia o arquivo klsq2.zip baixado para qualquer pasta no dispositivo com o Servidor de Administração do Kaspersky Security Center Linux instalado.

O pacote klsq2.zip inclui os seguintes arquivos:

- klsq2.exe
- src.sql
- start.cmd

3. Abra o arquivo src.sql em qualquer editor de texto.
4. No arquivo src.sql, digite a consulta SQL desejada e salve o arquivo.
5. No dispositivo com o Servidor de Administração do Kaspersky Security Center Linux instalado, na linha de comando, digite o seguinte comando para executar a consulta SQL do arquivo src.sql e salvar os resultados no arquivo result.xml:

```
klsq2 -i src.sql -o result.xml
```

6. Abra o arquivo result.xml recentemente criado para exibir os resultados da consulta.

Você pode editar o arquivo src.sql e criar qualquer consulta para as vistas públicas. Então, da linha de comando, execute a sua consulta e salve os resultados em um arquivo.

Exemplo de uma consulta SQL no utilitário klsq2

Esta seção mostra um exemplo de uma consulta SQL, criada por meio do utilitário klsq2.

O exemplo a seguir ilustra a recuperação dos eventos que ocorreram em dispositivos durante os últimos sete dias e exibe os eventos encomendados na hora de sua ocorrência, os eventos mais recentes são exibidos primeiro.

Exemplo:


```
SELECT
e.nId, /* identificador do evento */
e.tmRiseTime, /* hora, em que o evento ocorreu */
e.strEventType, /* nome interno do tipo de evento */
e.wstrEventTypeDisplayName, /* nome exibido do evento */
e.wstrDescription, /* descrição do evento exibida */
e.wstrGroupName, /* nome do grupo, onde o dispositivo está localizado */
h.wstrDisplayName, /* nome exibido do dispositivo, no qual o evento ocorreu */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* endereço IP do dispositivo, no qual
o evento ocorreu */
```

```
DE v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Exibir o nome de banco de dados do Kaspersky Security Center Linux

Se você deseja acessar o banco de dados do Kaspersky Security Center Linux por meio das ferramentas de gerenciamento de banco de dados do SQL Server, MySQL ou MariaDB deverá conhecer o nome do banco de dados para poder conectar-se ao mesmo a partir de seu editor de script SQL.

Para exibir o nome do banco de dados do Kaspersky Security Center Linux:

1. Clique no ícone **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 **Detalhes do banco de dados atual**.

O nome do banco de dados é especificado no campo **Nome do banco de dados**. Use o nome do banco de dados para endereçar o banco de dados nas suas consultas SQL.

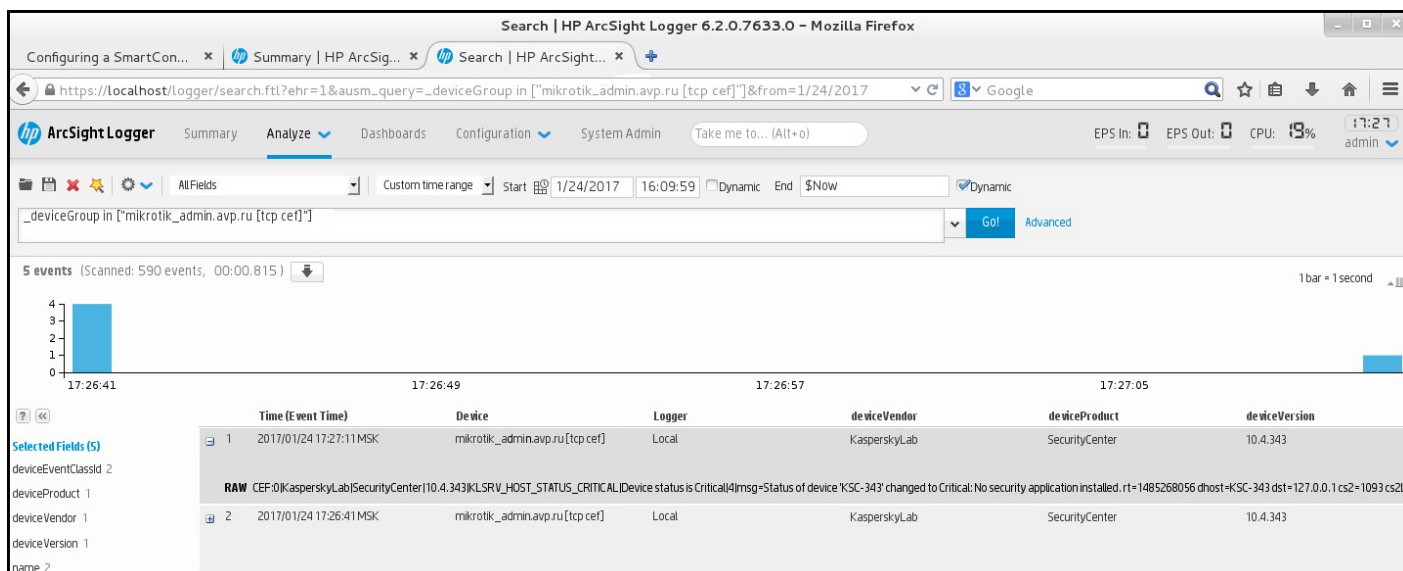
Exibir os resultados da exportação

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 Linux 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 Linux 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

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 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.

Para visualizar a seleção de dispositivos:

1. No menu principal, vá para a seção **DISPOSITIVOS** → **SELEÇÕES DE DISPOSITIVOS** ou **DESCOBERTA E IMPLEMENTAÇÃO** → **SELEÇÕES DE DISPOSITIVOS**.
2. Na lista de seleção, clique no nome da seleção relevante.

O resultado da seleção de dispositivos é exibido.

Criar uma seleção de dispositivos

Para criar uma seleção de dispositivos:

1. No menu principal, vá para **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 tipo de dispositivos que deseja incluir na seleções de dispositivo.

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. Acesse **DISPOSITIVOS** → **SELEÇÕES DE DISPOSITIVOS**.

Uma página com uma lista de seleções de dispositivos é exibida.

2. Clique na seleção de dispositivos definida pelo usuário relevante.

A janela **Configurações de seleção de dispositivos** se abre.

3. Na guia **Geral**, especifique as condições que devem ser atendidas para a inclusão de dispositivos nesta seleção.

4. 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.

Rede

Na seção **Rede**, você pode especificar o critério que será usado para incluir dispositivos na seleção de acordo com seus dados na rede:

- **Nome do dispositivo ou endereço IP**
- **[Domínio do Windows](#)** 

Exibe todos os dispositivos incluídos no grupo de trabalho 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 frases como **SUSE Linux Enterprise Server 12** ou **SUSE Linux Enterprise Server 15**, é possível inserir **SUSE Linux Enterprise Server 1?**.

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 IP](#) 

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.

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 todas as tags selecionadas.

Por padrão, esta opção está desativada.

- [A tag deve ser incluída](#) 

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.

- [A tag deve ser excluída](#) 

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.

Atividade de rede

Na seção **Atividade de rede**, você pode especificar o critério que será usado para incluir dispositivos na seleção de acordo com a sua atividade na rede:

- [Este dispositivo é um 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.** Os dispositivos que agem 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 inclui os dispositivos que se conectaram ao 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.

Aplicativo

Na seção **Aplicativo**, você pode configurar o critério para a inclusão de dispositivos em uma seleção com base no 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](#)**

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.

- **[Última atualização dos 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 através do Kaspersky Security Center 14](#)**

Na lista suspensa, você poderá incluir nos dispositivos selecionados gerenciados através do Kaspersky Security Center Linux:

- **Sim.** O aplicativo é incluído na seleção de dispositivos gerenciados através do Kaspersky Security Center Linux.
- **Não.** O aplicativo inclui na seleção os dispositivos que não são gerenciados através do Kaspersky Security Center Linux.
- **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 um aplicativo de segurança instalado.
- **Nenhum valor está selecionado.** O critério não será aplicado.

Sistema operacional

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.

- [Versão do sistema operacional](#) 

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.

- [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.

- [Versão do Service Pack do sistema operacional](#) 

Nesse campo, você poderá 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.

- [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.

- [ID 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.

Status do dispositivo

Na seção **Status do dispositivo**, você pode configurar o critério para a inclusão de dispositivos em uma seleção com base na 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*.

- [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*.

- [Status do dispositivo definido pelo aplicativo](#) ?

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.

Componentes de proteção

Na seção **Componentes de proteção**, você pode configurar critérios para a inclusão de dispositivos em uma seleção com base no seu status de proteção:

- [Versão dos bancos de dados](#) ?

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.

- [Última verificação](#) ?

Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pela hora da última verificação de vírus. No campo de entrada, você poderá especificar o período de tempo no qual a última verificação de vírus foi executada.

Por padrão, esta opção está desativada.

- [Número total de ameaças detectadas](#) ?

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.

Registro de aplicativos

Na seção **Registro de aplicativos**, você pode definir o critério para pesquisar por dispositivos de acordo com os aplicativos neles instalados:

- [Nome do aplicativo](#) ?

Lista suspensa na qual é possível selecionar um aplicativo. Os dispositivos nos quais o aplicativo 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 de 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.

Registro de hardware

Na seção **Registro de hardware**, você pode configurar o critério para a inclusão de dispositivos em uma seleção com base no seu hardware instalado:

- [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](#) 

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 formato 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 da CPU em MHz](#)**

O intervalo de frequência de uma CPU. Os dispositivos com CPU's que correspondem a faixa de frequência nesses campos (inclusive) serão incluídos na seleção.

- **[Núcleos de CPU virtuais](#)**

Faixa de número de núcleos virtuais em uma CPU. Os dispositivos com CPU's que correspondem a faixa de frequência nesses campos (inclusive) serão incluídos na seleção.

- **[Volume do disco rígido, em GB](#)**

Faixa de valores para o tamanho do disco rígido no dispositivo. Os dispositivos com discos rígidos que correspondem a faixa nesses campos de entrada (inclusive) serão incluídos na seleção.

- [Tamanho da RAM, em MB](#) 

Faixa de valores para o tamanho da RAM no dispositivo. Os dispositivos com memórias RAM que correspondam a faixa nesses campos de entrada (inclusive) serão incluídos na seleção.

Máquinas virtuais

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:

- **Irrelevante.**
- **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:

- **Irrelevante.**
- **Não.** Localizar dispositivos que não fazem parte da Virtual Desktop Infrastructure.
- **Sim.** Localizar dispositivos que fazem parte da Virtual Desktop Infrastructure (VDI).

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 esta opção estiver ativada, clique no botão **Procurar** para especificar uma conta de usuário. Os resultados da pesquisa incluem os dispositivos onde o usuário especificado efetuou o último login no sistema.

- [Usuário que fez login no sistema pelo menos uma vez](#) 

Se esta opção estiver ativada, clique no botão **Procurar** para especificar uma conta de usuário. Os resultados da pesquisa incluem os dispositivos nos quais o usuário especificado efetuou o login no sistema ao menos uma vez.

Problemas que afetam o status em aplicativos gerenciados

Na seção **Problemas que afetam o status em aplicativos gerenciados**, você pode 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.

[Descrição do status do dispositivo](#)

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.

Status dos componentes em aplicativos gerenciados

Na seção **Status dos componentes em aplicativos gerenciados**, você pode 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 de 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 de 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 Sensor de Endpoints](#) 

Procure dispositivos pelo status do componente Endpoint Sensor (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

Componentes do aplicativo

Esta seção contém a lista de componentes dos aplicativos que têm plugins de gerenciamento correspondentes instalados no Console de Administração.

Na seção **Componentes do aplicativo**, você pode especificar critérios para a inclusão de dispositivos em uma seleção segundo os status e os números da versão dos componentes que fazem referência ao aplicativo que você selecionar:

- **Status** 

Pesquise dispositivos segundo o status do componente enviado por um aplicativo ao Servidor de Administração. Você pode selecionar um dos seguintes status: *Nenhum dado do dispositivo*, *Interrompido*, *Iniciando*, *Pausado*, *Executando*, *Mau funcionamento*, ou *Não instalado*. 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:

- *Iniciando* – o componente está atualmente em processo de inicialização.
- *Executando* – o componente está ativado e funcionando corretamente.
- *Pausado* – o componente está suspenso, por exemplo, depois que o usuário pausou a proteção no aplicativo gerenciado.
- *Mau funcionamento* – um erro ocorreu durante a operação do componente.
- *Interrompido* – o componente está desativado e não está funcionando no momento atual.
- *Não instalado* – o usuário não selecionou o componente para instalação ao configurar a instalação personalizada do aplicativo.

Diferentemente de outros status, o status *Nenhum dado do dispositivo* 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.

Guia de referência de API

Este guia de referência da OpenAPI do Kaspersky Security Center foi projetado para ajudar nas seguintes tarefas:

- Automação e personalização. É possível automatizar tarefas que você não deseja tratar manualmente. Por exemplo, como administrador, é possível usar o Kaspersky Security Center OpenAPI para criar e executar scripts que facilitarão o desenvolvimento da estrutura dos grupos de administração e manterão essa estrutura atualizada.
- Desenvolvimento personalizado. Usando a OpenAPI, você pode desenvolver um aplicativo cliente.

É possível usar o campo de pesquisa à direita da tela para localizar as informações de que precisa no guia de referência da OpenAPI.



[GUIA DE REFERÊNCIA DA OPENAPI](#)

Exemplos de scripts

O guia de referência do OpenAPI contém exemplos dos scripts Python listados na tabela abaixo. Os exemplos mostram como você pode chamar métodos OpenAPI e realizar automaticamente várias tarefas para proteger sua rede, por exemplo, criar uma [hierarquia "principal/secundária"](#), executar [tarefas](#) no Kaspersky Security Center ou atribuir [pontos de distribuição](#). Você pode executar as amostras como estão ou criar seus próprios scripts com base nos exemplos.

Para chamar os métodos OpenAPI e executar scripts:

1. [Baixe o arquivo KIAkOAPI.tar.gz](#). Este arquivo inclui o pacote e exemplos KIAkOAPI (você pode copiá-los do arquivo ou do guia de referência OpenAPI).
2. [Instale o pacote KIAkOAPI](#) do arquivo KIAkOAPI.tar.gz em um dispositivo onde o Servidor de Administração está instalado.

Você poderá chamar os métodos OpenAPI, executar os exemplos e seus próprios scripts somente em dispositivos onde o Servidor de Administração e o pacote KIAkOAPI estiverem instalados.

Correspondência entre cenários de usuário e exemplos de métodos de OpenAPI do Kaspersky Security Center

Exemplo	Objetivo do exemplo	Cenário
Log KIAkParams	É possível extrair e processar dados usando a estrutura de dados KIAkParams. O exemplo mostra como trabalhar com essa estrutura de dados. A saída, nesse exemplo, pode estar presente de maneiras diferentes. É possível obter os dados para enviar um método HTTP ou para usar em seu código.	Monitoramento e relatórios
Criar e excluir uma hierarquia primária/secundária	Você pode adicionar um Servidor de Administração secundário e estabelecer uma hierarquia "primária/secundária". Como alternativa, é possível desconectar o Servidor de Administração secundário da hierarquia.	Como criar uma hierarquia de Servidores de Administração, adicionando um Servidor de Administração secundário e como excluir uma hierarquia de Servidores de Administração
Baixar arquivos de lista de rede por meio do	É possível conectar o Agente de Rede no dispositivo necessário usando um gateway de	Ajuste de pontos de distribuição e gateways de

gateway de conexão para o host especificado	conexão e depois baixar um arquivo com a lista de redes no computador.	conexão
Instalar uma chave de licença armazenada no repositório principal do Servidor de Administração nos Servidores de Administração secundários	É possível se conectar ao Servidor de Administração principal, baixar uma chave de licença necessária a partir dele e transmitir essa chave para todos os Servidores de Administração secundários incluídos em uma hierarquia.	Licenciamento de aplicativos gerenciados
Criar um relatório de direitos efetivos do usuário	É possível criar relatórios diferentes . Por exemplo, é possível gerar o relatório dos direitos efetivos do usuário usando este exemplo. Este relatório descreve os direitos de um usuário, dependendo do seu grupo e função. É possível baixar o relatório no formato HTML, PDF ou Excel.	Como gerar e visualizar um relatório
Iniciar a tarefa do dispositivo	É possível se conectar ao Agente de Rede no dispositivo necessário usando um gateway de conexão e executar na sequência a tarefa necessária.	Como iniciar uma tarefa manualmente
Registrar os pontos de distribuição para dispositivos em um grupo	É possível atribuir dispositivos gerenciados como pontos de distribuição (anteriormente conhecidos como agentes de atualização).	Atualização dos bancos de dados e dos aplicativos da Kaspersky
Enumerar todos os grupos	É possível executar as seguintes ações nos grupos de administração: No exemplo é mostrado como fazer o seguinte: <ul style="list-style-type: none"> • Obtenha um identificador do grupo raiz "Dispositivos gerenciados" • Percorra a hierarquia do grupo • Recupere a hierarquia completa e expandida de grupos, junto com seus nomes e aninhamento 	Configurando o Servidor de Administração
Enumerar tarefas, consultar estatísticas de tarefas e executar uma tarefa	É possível descobrir as seguintes informações: <ul style="list-style-type: none"> • Histórico de progresso da tarefa • Status da tarefa atual • Número de tarefas em diferentes status É possível também executar uma tarefa. Por padrão, a amostra executa uma tarefa depois de gerar estatísticas.	Monitoramento de execução de tarefa
Criar e executar uma tarefa	É possível criar uma tarefa. Especifique os seguintes parâmetros de tarefa no exemplo: <ul style="list-style-type: none"> • Tipo 	Criar uma tarefa

	<ul style="list-style-type: none"> • Método de execução • Nome • Grupo de dispositivos para o qual a tarefa será usada <p>Por padrão, no exemplo é criada uma tarefa do tipo "Mostrar mensagem". É possível executar esta tarefa para todos os dispositivos gerenciados do Servidor de Administração. Se necessário, é possível especificar seus próprios parâmetros de tarefa.</p>	
Enumerar chaves de licença	É possível obter uma lista de todas as chaves de licença ativas para os aplicativos Kaspersky instalados em dispositivos gerenciados do Servidor de Administração. A lista contém dados detalhados sobre cada chave de licença, como nome, tipo ou data de expiração.	Visualizando de informações sobre chaves de licença em uso
Criar e encontrar um usuário interno	É possível criar uma conta para trabalhos futuros.	Selecionar a conta para iniciar o Servidor de Administração
Criar uma categoria personalizada	É possível criar a categoria do aplicativo com os parâmetros necessários.	Criar uma categoria de aplicativos com conteúdo adicionado manualmente
Enumerar usuários usando SrvView	É possível usar a classe SrvView para solicitar informações detalhadas do Servidor de Administração. Por exemplo, é possível obter uma lista de usuários usando este exemplo.	Como gerenciar contas de usuário

Aplicativos que interagem com o Kaspersky Security Center via OpenAPI

Alguns aplicativos interagem com o Kaspersky Security Center via OpenAPI. Esses aplicativos incluem, por exemplo, Kaspersky Anti Targeted Attack Platform ou Kaspersky Security for Virtualization. Também pode ser um aplicativo cliente personalizado, desenvolvido por terceiros, baseado em OpenAPI.

Os aplicativos que interagem com o Kaspersky Security Center via OpenAPI conectam-se ao Servidor de Administração. Caso tenha configurado uma [lista de permissão de endereços IP](#) para se conectar ao Servidor de Administração, adicione os endereços IP de dispositivos nos quais os aplicativos que usam o Kaspersky Security Center OpenAPI estão instalados. Para saber se o aplicativo usado funciona por OpenAPI, consulte a Ajuda do aplicativo.

Integração entre o Kaspersky Security Center Web Console e outras soluções

Esta seção descreve como configurar o acesso do Kaspersky Security Center Web Console a outro aplicativo Kaspersky, como o Kaspersky Endpoint Detection and Response e o Kaspersky Managed Detection and Response.

Configurar o acesso ao Console da Web KATA / KEDR

O Kaspersky Anti Targeted Attack (KATA) e o Kaspersky Endpoint Detection and Response (KEDR) são dois blocos funcionais da [Kaspersky Anti Targeted Attack Platform](#). Você pode gerenciar esses blocos funcionais através do Console da Web da Kaspersky Anti Targeted Attack Platform (KATA / KEDR Web Console). Se você usar o Kaspersky Security Center 14 Web Console e o KATA / KEDR Web Console, poderá configurar o acesso ao KATA / KEDR Web Console diretamente da interface do Kaspersky Security Center 14 Web Console.

Para configurar o acesso ao KATA / KEDR Web Console:

1. Na janela principal do aplicativo, clique em **Configurações do console** na parte superior da tela.
2. No menu suspenso, selecione **Integração**.
A janela Configurações do console se abre.
3. No guia **Integração**, digite a URL do URL of KATA/KEDR Web Console no campo **URL para KATA/KEDR Web Console**.
4. Clique no botão **Salvar**.

A lista suspensa **Gerenciamento avançado** é adicionada à parte superior da janela principal do aplicativo. Você pode usar este menu para abrir o KATA / KEDR Web Console. Depois de clicar em **Advanced Cybersecurity Platform**, uma nova guia é aberta no navegador com a URL especificada.

Estabelecendo uma conexão em segundo plano

Para configurar a interação entre o Kaspersky Security Center e outro aplicativo ou solução da Kaspersky, por exemplo, o [Kaspersky Managed Detection and Response](#) (também conhecido como MDR), você deve estabelecer uma conexão de segundo plano entre o Kaspersky Security Center Web Console e o Servidor de Administração. É possível estabelecer esta conexão somente se a conta tiver o direito de Modificar ACLs de objeto na área funcional **Recursos gerais: permissões de usuário**.

É possível configurar a interação apenas entre o Kaspersky Managed Detection and Response e a versão baseada no Windows do Kaspersky Security Center.

Para estabelecer uma conexão em segundo plano:

1. Na lista suspensa **Configurações do console**, selecione **Integração**.
A janela **Configurações do console** se abre.
2. Selecione a guia **Integração**.

3. Na guia **Integração**, selecione a seção **Integração**.
4. Alterne o botão para estabelecer uma conexão em segundo plano para a posição: **Estabelecer uma conexão em segundo plano para integração ATIVADO**.
5. Na seção aberta **O serviço que estabelece uma conexão em segundo plano será iniciado no Kaspersky Security Center Web Console Server está instalado**, clique no botão **OK**.

A conexão de segundo plano entre o Kaspersky Security Center Web Console e o Servidor de Administração é estabelecida. O Servidor de Administração cria uma conta para a conexão em segundo plano e essa conta é usada como uma conta de serviço para manter a interação entre o Kaspersky Security Center e outro aplicativo ou solução Kaspersky. O nome desta conta de serviço contém o prefixo NWCSvcUser. Por motivos de segurança, o Servidor de Administração muda automaticamente a senha da conta de serviço a cada 30 dias. Você não pode excluir a conta de serviço manualmente. O Servidor de Administração exclui esta conta automaticamente se você desativar uma conexão entre serviços. O Servidor de Administração cria uma única conta de serviço para cada Kaspersky Security Center 14 Web Console e Console de Administração e atribui todas as contas de serviço ao grupo de segurança com o nome ServiceNwcGroup. O Servidor de Administração cria este grupo de segurança automaticamente durante o processo de instalação do Kaspersky Security Center. Você não pode excluir este grupo de segurança manualmente.

Contatar o Suporte Técnico

Esta seção descreve como adquirir o suporte técnico e os termos com os quais está disponível.

Como obter suporte técnico

Caso não consiga encontrar uma solução para o problema na documentação do Kaspersky Security Center Linux ou em nenhuma das fontes de informação sobre Kaspersky Security Center Linux, contate o Suporte Técnico. Os especialistas do Suporte Técnico responderão a todas as suas dúvidas sobre instalação e uso do Kaspersky Security Center Linux.

A Kaspersky fornece suporte para O Kaspersky Security Center Linux 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](#)

Obter suporte técnico por telefone

Você pode ligar para os especialistas do Suporte Técnico a partir da maioria das regiões ao redor do mundo. É possível encontrar as informações para obter suporte técnico na sua região e informações de contato para Suporte Técnico no [site de Serviço ao Cliente da Kaspersky](#).

Antes de entrar em contato com o Serviço de Suporte Técnico, leia as [regras de suporte](#).

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](#).

Fontes de informação sobre o aplicativo

Página do Kaspersky Security Center no site da Kaspersky

Na [página do Kaspersky Security Center no site da Kaspersky](#), é possível exibir informações gerais sobre o aplicativo, suas funções e recursos.

Página do Kaspersky Security Center 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 Linux na Base de conhecimento](#), é possível ler artigos que fornecem informações úteis, recomendações e respostas às perguntas frequentes sobre como comprar, instalar e usar o aplicativo.

Os artigos na Base de Dados de Conhecimento podem fornecer respostas às perguntas relacionadas ao Kaspersky Security Center como também a outros aplicativos 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 Linux tem uma série de limitações que não são críticas para a operação do aplicativo:

- Na tarefa *Baixar atualizações no repositório do Servidor de Administração* e na tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a autenticação do usuário não funcionará se for selecionada uma pasta local ou de rede protegida por senha como fonte de atualização. Para resolver esse problema, primeiro monte a pasta protegida por senha e, em seguida, especifique as credenciais necessárias, por exemplo, por meio do sistema operacional. Depois disso, será possível selecionar essa pasta como fonte de atualização em uma tarefa de download de atualizações. O Kaspersky Security Center não solicitará a inserção das credenciais.
- A tarefa *Alterar Servidor de Administração* não inicia automaticamente depois que a opção **Imediatamente** for definida na agenda de tarefas e as alterações forem salvas.
- Se forem especificadas as configurações do servidor proxy nas propriedades do Servidor de Administração e, em seguida, for ativada a opção **Não usar o servidor proxy** na tarefa *Baixar atualizações no repositório do Servidor de Administração*, essa opção será ignorada e a conexão é estabelecida por meio do servidor proxy.
- Se o Kaspersky Security Center 14 Web Console for aberto em navegadores diferentes e for baixado o arquivo de certificado do Servidor de Administração na janela de propriedades do Servidor de Administração, os arquivos baixados terão nomes diferentes.
- Ocorre um erro ao tentar restaurar um objeto do repositório **BACKUP (OPERAÇÕES → REPOSITÓRIOS → BACKUP)** ou enviar o objeto para a Kaspersky.
- As configurações bloqueadas em uma política principal do Kaspersky Endpoint Security for Linux são herdadas, mas não bloqueadas nas políticas secundárias.
- As informações de hardware enviadas de um dispositivo gerenciado para o Servidor de Administração podem não estar completas; alguns itens de hardware podem não ser especificados.
- Uma categoria de aplicativo que você adicionou ao recurso Controle de aplicativos na política do Kaspersky Endpoint Security for Linux pode ser excluída.
- Um dispositivo gerenciado que possui mais de um adaptador de rede envia informações ao Servidor de Administração sobre o endereço MAC do adaptador de rede que não é aquele usado para se conectar ao Servidor de Administração.
- Se você especificar contas de usuário personalizadas nos parâmetros `webConsoleAccount` e `managementServiceAccount` em um arquivo de resposta para a instalação do Kaspersky Security Center 14 Web Console e essas contas pertencerem a grupos de segurança diferentes, o Kaspersky Security Center 14 Web Console não funcionará após a instalação.
- Na edição Astra Linux de 64 bits, o pacote `klagent-astra` não pode ser atualizado com o pacote `klagent64_14`: o pacote antigo `klagent64-astra` será removido e o novo pacote `klagent64` será instalado em vez da atualização, então o novo ícone para o dispositivo com o pacote `klagent64_14` será adicionado. É possível remover o ícone antigo deste dispositivo.

Glossário

Administrador cliente

Um membro da equipe de uma empresa cliente que é responsável por monitorar o status da proteção antivírus.

Administrador do Kaspersky Security Center

A pessoa que gerencia a operação de aplicativos através do sistema Kaspersky Security Center de administração centralizada remota.

Administrador do provedor de serviço

Um membro da equipe em um provedor de serviço de proteção antivírus. Esse administrador efetua tarefas de instalação e manutenção em sistemas de proteção antivírus com base em produtos da Kaspersky e também fornece suporte técnico a clientes.

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 que permite a interação entre o Servidor de Administração e os aplicativos Kaspersky instalados em um nó específico da rede (estação de trabalho ou servidor). Este componente é comum para 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 Linux.

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.

Atualização disponível

Um conjunto de atualizações dos módulos de aplicativo da Kaspersky com atualizações críticas acumuladas por um determinado período e alterações à arquitetura do aplicativo.

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.

Backup de dados do Servidor de Administração

Cópia dos dados do Servidor de Administração para backup e subsequente restauração realizada, usando o utilitário de backup. O utilitário pode salvar:

- O banco de dados do Servidor de Administração (políticas, tarefas, configurações de aplicativo, eventos salvos no Servidor de Administração)
- Informações de configuração sobre a estrutura dos grupos de administração e dispositivos cliente
- Repositório dos arquivos de instalação para instalação remota de aplicativos (conteúdo das pastas: Pacotes, Atualizações de Desinstalação)
- Certificado do Servidor de Administração

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.

Certificado compartilhado

Um certificado destinado a identificar o dispositivo móvel do usuário.

Certificado do Servidor de Administração

O certificado que o Servidor de Administração usa para os seguintes propósitos:

- Autenticação de Servidor de Administração ao conectar-se ao Kaspersky Security Center 14 Web Console
- Interação segura entre o Servidor de Administração e os Agentes de Rede em dispositivos gerenciados

- Autenticação de Servidores de Administração ao conectar um Servidor de Administração principal a um Servidor de Administração secundário

O certificado é criado automaticamente quando o servidor de administração é instalado e, a seguir, armazenado no servidor de administração.

Chave ativa

Uma chave usada atualmente pelo aplicativo.

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 Administração

Um componente do Kaspersky Security Center baseado no Windows (também chamado de Console de Administração baseado em MMC). Este componente fornece uma interface de usuário para os serviços administrativos do Servidor de Administração e do Agente de Rede. O Console de Administração é um análogo do Kaspersky Security Center 14 Web Console.

Direitos de administrador

O nível de direitos e privilégios do usuário para administração de objetos Exchange numa organização Exchange.

Dispositivos gerenciados

Dispositivos na rede corporativa que estão incluídos em um grupo de administração.

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).

Estação de trabalho do administrador

Um dispositivo do qual você abre o Kaspersky Security Center 14 Web Console. Este componente fornece uma interface de gerenciamento do Kaspersky Security Center.

A estação de trabalho do administrador é usada para configurar e gerenciar o lado do servidor do Kaspersky Security Center. Usando a estação de trabalho, o administrador cria e gerencia um sistema centralizado de proteção antivírus para uma LAN corporativa, com base em aplicativos Kaspersky.

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.

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.

Grupo de aplicativos licenciados

Um grupo de aplicativos criado com base no critério definido pelo administrador (por exemplo, por fornecedor), para o qual as estatísticas de instalações dos dispositivos cliente são mantidas.

Grupo de funções

Um grupo de usuários de dispositivos móveis Exchange ActiveSync que recebem [direitos de administrador](#) idênticos.

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.

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 manual

A instalação de um aplicativo de segurança em um dispositivo na rede corporativa do pacote de distribuição. A instalação manual requer uma participação de um administrador ou outro especialista de TI. A instalação manual típica é efetuada caso a instalação remota tenha sido concluída com um erro.

Instalação remota

Instalação de aplicativos Kaspersky usando os serviços fornecidos pelo Kaspersky Security Center Linux.

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 (KSN Privada)

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 do usuário 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.

Loja de aplicativos

Componente do Kaspersky Security Center. A Loja de aplicativos é usada para instalar aplicativos em dispositivos Android possuídos por usuários. A Loja de aplicativos permite publicar os arquivos APK de aplicativos e os links aos aplicativos no Google Play.

Operador do Kaspersky Security Center

Usuário que monitora o status e operação de um sistema de proteção gerenciado através do Kaspersky Security Center.

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. 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.

Pasta de backup

Pasta especial para armazenamento das cópias de dados do Servidor de Administração criados usando o utilitário de backup.

Perfil

Um conjunto de configurações de [Dispositivos móveis Exchange](#) que define seu comportamento quando conectado a um Microsoft Exchange Server.

Perfil de configuração

Política que contém um conjunto de configurações e restrições para um dispositivo móvel MDM do iOS.

Perfil de provisionamento

Conjunto de configurações para operação de aplicativos em dispositivos móveis iOS. Um perfil de provisionamento contém informações sobre a licença. Está associado a um aplicativo em específico.

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.

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 um Agente de Rede instalado e é usado para a distribuição da atualização, instalação remota de aplicativos, obtenção de informações sobre os computadores em um grupo de administração e/ou domínio de broadcasting. Os pontos de distribuição são projetados para reduzir a carga no Servidor de Administração durante a distribuição da atualização e para otimizar o tráfego na rede. Os pontos de distribuição podem ser atribuídos automaticamente pelo Servidor de Administração ou manualmente pelo administrador. O ponto de distribuição era anteriormente conhecido como agente de atualização.

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.

Provedor de serviço de proteção antivírus

Uma organização que fornece a uma organização cliente serviços de proteção antivírus com base nas soluções da Kaspersky.

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 Linux.

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.

Restauração dos dados do Servidor de Administração

Restauração dos dados do Servidor de Administração a partir de informações salvas na cópia backup usando o utilitário de backup. O utilitário pode restaurar:

- O banco de dados do Servidor de Administração (políticas, tarefas, configurações de aplicativo, eventos salvos no Servidor de Administração)
- Informações de configuração sobre a estrutura dos grupos de administração e computadores cliente
- Repositório dos arquivos de instalação para instalação remota de aplicativos (conteúdo das pastas: Pacotes, Atualizações de Desinstalação)
- Certificado do Servidor de Administração

Servidor de Administração

Um componente do Kaspersky Security Center que armazena centralmente informações sobre todos os aplicativos Kaspersky instalados na rede empresarial. Pode também ser usado para gerenciar estes aplicativos.

Servidor de Administração cliente (Dispositivo cliente)

Um dispositivo, servidor ou estação de trabalho no qual o Agente de Rede está instalado e os aplicativos Kaspersky gerenciados estão em execução.

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 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:

- O Servidor de Administração virtual só pode ser criado no Servidor de Administração principal.
- O Servidor de Administração virtual usa o banco de dados do Servidor de Administração principal. Tarefas de backup e restauração de dados, bem como tarefas de verificação de atualização e download, não são compatíveis com um Servidor de Administração virtual.
- O Servidor virtual não é compatível com a criação de Servidores de Administração secundários (incluindo Servidores virtuais).

Servidor Web do Kaspersky Security Center

Um componente do Kaspersky Security Center que é instalado em conjunto com o Servidor de Administração. O Servidor da Web foi projetado para a transmissão, através de uma rede, de pacotes de instalação independentes, perfis MDM do iOS e arquivos de uma pasta compartilhada.

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.

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.

Usuários internos

As contas dos usuários internos são usadas para trabalhar com os Servidores de Administração virtuais. O Kaspersky Security Center concede direitos de usuários reais a usuários internos do aplicativo.

As contas de usuários internos só são criadas e usadas dentro do Kaspersky Security Center. Os dados sobre os usuários internos não são transferidos para o sistema operacional. O Kaspersky Security Center autentica os usuários internos.

Validador de Integridade do Sistema do Kaspersky Security Center (SHV)

Um componente do Kaspersky Security Center concebido para verificar a operabilidade do sistema operacional em caso da operação simultânea do Kaspersky Security Center e do Microsoft NAP.

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 podem ser encontradas no arquivo `legal_notices.txt` e armazenadas no diretório de instalação do aplicativo.

Avisos de marca registrada

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

Adobe, Acrobat, Flash Shockwave e PostScript são marcas comerciais registradas ou marcas comerciais da Adobe nos Estados Unidos e/ou outros países.

AMD, AMD64 são marcas comerciais ou marcas registradas da Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace são marcas comerciais da Amazon.com, Inc. ou de suas afiliadas nos Estados Unidos e/ou em outros países.

Apache e o logotipo da pena Apache são marcas comerciais propriedade da The Apache Software Foundation.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime e Touch ID são marcas comerciais da Apple Inc. registradas nos Estados Unidos e em outros países e regiões.

A palavra, marca e os logótipos Bluetooth são propriedade da Bluetooth SIG, Inc.

Ubuntu é uma marca comercial registrada da Canonical Ltd.

Cisco, Cisco Systems, iOS são marcas comerciais registradas ou marcas comerciais propriedade da Cisco Systems, Inc. e/ou seus afiliados nos Estados Unidos e 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.

Corel é uma marca comercial ou marca comercial registrada 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.

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, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts e YouTube são marcas comerciais da Google LLC.

FusionCompute, FusionSphere são marcas comerciais da Huawei Technologies Co., Ltd, registradas na China e em outros países.

Intel, Core, Xeon 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.

Micro Focus é uma marca comercial ou marca comercial registrada da Micro Focus (IP) Limited ou de suas subsidiárias no Reino Unido, Estados Unidos e outros países.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista e Windows Azure são marcas comerciais registradas do grupo de empresas da Microsoft.

Mozilla, Firefox, Thunderbird são marcas comerciais da Mozilla Foundation.

Novell é uma marca comercial registrada da Novell Enterprises Inc. nos Estados Unidos e em outros países.

Oracle, Java, JavaScript e TouchDown são marcas comerciais registradas da Oracle e/ou suas afiliadas.

Parallels e o logotipo da Parallels são marcas comerciais ou marcas registradas da Parallels International GmbH no Canadá, Estados Unidos e/ou em outros lugares.

Chef é uma marca comercial ou marca registrada da Progress Software Corporation e/ou uma de suas subsidiárias ou afiliadas nos EUA e/ou em outros países.

Puppet é uma marca comercial ou marca registrada da Puppet, Inc.

Python é uma marca comercial ou marca registrada da Python Software Foundation.

Red Hat, Ansible, CentOS, Fedora e Red Hat Enterprise Linux são marcas comerciais da Red Hat Inc. ou de suas subsidiárias registradas 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.

Debian é uma marca registrada da Software in the Public Interest, Inc.

Splunk, SPL são marcas comerciais e marcas comerciais registradas 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.

OpenAPI é uma marca registrada da Linux Foundation.

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.

Zabbix é uma marca comercial registrada da Zabbix SIA.