kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Índice

Sobre o Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Esta seção descreve as funções, os componentes e o kit de distribuição do Kaspersky Endpoint Security, e fornece uma lista de requisitos de hardware e software do Kaspersky Endpoint Security.

Novidades

O Kaspersky Endpoint Security 10 Service Pack 2 for Windows oferece os seguintes recursos e melhorias:

1. Controle de Inicialização de Aplicativo:
   - Suporte a sistemas operacionais de servidor.
   - Controle de downloads de módulos DLL e drivers.
   - Gerencia a lista de objetos na tarefa de inventário (módulos de DLL e arquivos de script).
   - Controle de objetos com base em um novo critério - por atributos de certificados de assinatura digital.
   - Gera um relatório sobre inícios de teste de aplicativos bloqueados.
   - Suporta dois modos operacionais para Controle de Inicialização de Aplicativo: “Lista negra” e “Lista branca”.
   - Usa o hash SHA256 para controlar e inventariar objetos.
   - Controla a execução de scripts do interpretador do PowerShell.
   - Utiliza armazenamento de certificado de sistema confiável.
2. A administração do Microsoft BitLocker ativa a criptografia dos discos rígidos com a ajuda da tecnologia BitLocker da Microsoft:
   - Gerenciar remotamente a criptografia.
   - Monitorar dispositivos criptografados.
   - Criar relatórios de criptografia de dispositivos.
   - Restaurar o acesso a dispositivos criptografados.
3. Kaspersky Disk Encryption:
   - Suporte para entrada das credenciais no ambiente de pré-inicialização do Agente de Autenticação usando um teclado virtual.
   - O suporte do modo de criptografia para criptografia somente ocupou espaço em um dispositivo.
   - Suporte para criptografia em tablets (MS Surface versões 3 e 4).
4. Controle de Privilégios de Aplicativo:
   - Controla o acesso de aplicativos para dispositivos de gravação de áudio e vídeo.

5. Controle da Web:

   - Configura regras de acesso a recursos da Web para categorias adicionais de recursos da Web.

6. Controle de Dispositivo:

   - Registra eventos associados a exclusão e salvamento de arquivos em dispositivos USB.
   - Gera uma lista de redes Wi-Fi confiáveis com base nas seguintes configurações: nome, tipo de criptografia e tipo de autenticação.
   - Gerencia direitos de acesso de usuário para operações de leitura e gravação de arquivo em discos CD/DVD.

7. Antivírus de E-mail:

   - Capaz de excluir e renomear tipos específicos de arquivos dentro de arquivos compactados para verificação pelo Antivírus de e-mail.

8. Kaspersky Security Network:

   - Exibe o KSN como um motivo de uma decisão quanto ao método de processamento de objeto em relatórios do Kaspersky Endpoint Security e do Kaspersky Security Center.
   - Envia uma pergunta ao KSN quanto à reputação de um arquivo selecionado.
   - Exibe o status da disponibilidade dos servidores KSN para computadores clientes com o Kaspersky Endpoint Security instalado.

Kit de distribuição

O kit de distribuição do Kaspersky Endpoint Security contém os seguintes arquivos:

- Os arquivos necessários para a instalação do aplicativo usando diversos métodos disponíveis.
- Atualizar arquivos de pacote usados durante a instalação do aplicativo.
- O arquivo klcfginst.msi para a instalação do plug-in de administração do Kaspersky Endpoint Security via Kaspersky Security Center.
- O arquivo ksn_<ID de idioma>.txt, com o qual você pode exibir os termos da participação no Kaspersky Security Network.
- O arquivo license.txt, com o qual você pode exibir o Contrato de Licença de Usuário Final.
- O arquivo incompatible.txt que contém uma lista de software incompatível.
- O arquivo installer.ini que contém as configurações internas do kit de distribuição.

> Não se recomenda modificar os valores dessas configurações. Se desejar modificar as opções Instalação, use o arquivo setup.ini.

Você deve descompactar o kit de distribuição para acessar os arquivos.

Organizar a proteção do computador

O Kaspersky Endpoint Security oferece proteção abrangente do computador contra vários tipos de ameaças, ataques de rede e de phishing.

Cada tipo de ameaça é processada por um componente exclusivo. É possível ativar e desativar os componentes, como também configurá-los, sem que haja dependência entre eles.

Embora os componentes do aplicativo ofereçam proteção em tempo real, é recomendável *verificar* o computador regularmente para detectar vírus e outras ameaças. Esta ação é necessária para eliminar a possibilidade de contaminação por malware que não é detectado pelos componentes de proteção devido à existência de um nível de segurança baixo ou por outros motivos.

Para manter o Kaspersky Endpoint Security atualizado, é necessário *atualizar* os bancos de dados e módulos do aplicativo. O aplicativo é atualizado automaticamente por padrão, mas também é possível atualizar os bancos de dados e módulos do aplicativo manualmente se preferir.

Os seguintes componentes do aplicativo são componentes de controle:

- **Controle de Inicialização de Aplicativo**. Este componente monitora as tentativas do usuário de iniciar aplicativos e controla a inicialização de aplicativos.

- **Controle de Privilégios de Aplicativo**. Este componente faz o registro das ações dos aplicativos no sistema operacional e controla a atividade do aplicativo de acordo com o grupo confiável de um aplicativo específico. É especificado um conjunto de regras para cada grupo de aplicativos. Estas regras controlam o acesso de aplicativos aos dados do usuário e aos recursos do sistema operacional. Estes dados incluem os arquivos do usuário (pasta Meus Documentos, cookies, informações sobre as ações do usuário) e arquivos, pastas e chaves de registro que contêm configurações e informações importantes dos aplicativos utilizados com mais frequência.

- **Monitoramento de Vulnerabilidades**. O componente Monitoramento de Vulnerabilidades executa a verificação de vulnerabilidades, em tempo real, de aplicativos que foram executados ou que estão em execução no computador do usuário.

- **Controle de Dispositivo**. Este componente permite definir restrições adaptáveis de acesso a dispositivos de armazenamento de dados (como discos rígidos, unidades removíveis, unidades de fita e discos CD e DVD), equipamento de transmissão de dados (como modens), equipamentos de leitura direta (como impressoras) ou interfaces de conexão de dispositivos a computadores (como USB, Bluetooth e Infravermelho).

- **Controle da Web**. Este componente permite a definição de restrições adaptáveis de acesso a recursos da Web para grupos de usuários diversos.

O processamento dos componentes de controle baseia-se nas seguintes regras:

- Controle de Inicialização de Aplicativo usa Regras de Controle de Inicialização de Aplicativos

- Controle de Privilégios de Aplicativo usa regras de Controle de Aplicativos.

- O Controle de Dispositivo usa regras de acesso a dispositivo e regras de acesso a barramento de conexão.

- O Controle da Web usa regras de acesso a recurso da Web.

A seguir estão os componentes do aplicativo de proteção:

- **Antivírus de Arquivos**. Este componente protege o sistema de arquivos do computador de infecções. O Antivírus de Arquivos inicia juntamente com o Kaspersky Endpoint Security, permanece ativo na memória do computador e verifica todos os arquivos que são abertos, salvos ou executados no computador, em todas as unidades ativas. O Antivírus de Arquivos intercepta todas as tentativas de acesso a arquivos e verifica o arquivo para detectar vírus e outras ameaças.

- **Inspetor do Sistema**. Este componente registra a atividade de aplicativos no computador e fornece essa informação a outros componentes, a fim de garantir proteção ideal ao computador.

- **Antivírus de E-mail**. Este componente verifica as mensagens de e-mail recebidas e enviadas para detectar vírus e outras ameaças.

- **Antivírus da Web**. Este componente verifica o tráfego que chega ao computador do usuário através dos protocolos HTTP e FTP, e verifica se os URLs estão listados como endereços da Web maliciosos ou de phishing.

- **Antivírus de MI**. Este componente verifica o tráfego que chega ao computador através dos protocolos de clientes de MI. O componente permite que você use com segurança muitos clientes de MI.

- **Firewall**. Esse componente protege os dados que estão armazenados no computador e bloqueia a maioria dos tipos de ameaças ao sistema operacional enquanto o computador está conectado à Internet ou a uma rede local. O componente filtra toda a atividade de rede segundo regras de dois tipos: regras de rede para aplicativos e regras de pacote de rede.

- **Monitor de Rede**. Este componente permite exibir a atividade de rede do computador em tempo real.

- **Bloqueio de Ataque de Rede**. Este componente examina o tráfego de rede de entrada para detectar atividades típicas de ataques de rede. Ao detectar uma tentativa de ataque de rede ao computador, o Kaspersky Endpoint Security bloqueia a atividade de rede do computador em ataque.

O Kaspersky Endpoint Security disponibiliza as seguintes tarefas:

- **Verificação Completa**. O Kaspersky Endpoint Security verifica o sistema operacional, incluindo a memória RAM, objetos carregados na inicialização, armazenamento de backup do sistema operacional e todos os discos rígidos e unidades removíveis.

- **Verificação Personalizada**. O Kaspersky Endpoint Security verifica os objetos que foram selecionados pelo usuário.

- **Verificação de Áreas Críticas**. O Kaspersky Endpoint Security verifica os objetos carregados na inicialização do sistema operacional, da RAM e de objetos que são alvos de rootkits.

- **Atualização**. O Kaspersky Endpoint Security baixa bancos de dados e módulos do aplicativo atualizados. A atualização mantém o computador protegido contra os últimos vírus e outras ameaças.

- **Verificação de vulnerabilidades**. O Kaspersky Endpoint Security verifica o sistema operacional e o software instalado para detectar vulnerabilidades. A verificação garante a detecção e eliminação de possíveis problemas, que invasores podem usar em seu benefício, em tempo hábil.

A funcionalidade de criptografia de arquivos permite que você criptografe arquivos e pastas que estão armazenados nas unidades do computador local. A funcionalidade de criptografia da unidade permite a criptografia de discos rígidos e de unidades removíveis.

Administração remota no Kaspersky Security Center

Com o Kaspersky Security Center, é possível iniciar e encerrar o Kaspersky Endpoint Security de forma remota no computador cliente, e gerenciar e definir remotamente as configurações do aplicativo.

Funções de serviço do aplicativo

O Kaspersky Endpoint Security inclui um número de funções de serviço. As funções do serviço destinam-se a manter o aplicativo atualizado, aumentar sua funcionalidade e ajudar o usuário a operá-lo.

- **Relatórios**. Durante sua execução, o aplicativo apresenta um relatório de todos seus componentes e tarefas. O relatório contém uma lista de eventos do Kaspersky Endpoint Security e de todas as operações do aplicativo. É possível enviar os relatórios à Kaspersky se houver algum evento, para que os especialistas do Suporte Técnico possam analisar o evento de forma aprofundada.

- **Armazenamento de dados**. Se o aplicativo detectar arquivos infectados ou provavelmente infectados durante a verificação do computador para detectar vírus e outras ameaças, ele bloqueará estes arquivos. O Kaspersky Endpoint Security coloca os arquivos provavelmente infectados em um local de armazenamento especial, a *Quarentena*. O Kaspersky Endpoint Security armazena as cópias de arquivos desinfectados e excluídos no *Backup*. O Kaspersky Endpoint Security move os arquivos que não foram processados por qualquer motivo para a *lista de arquivos não processados*. Você pode verificar arquivos, restaurar arquivos para as pastas de origem e esvaziar o armazenamento de dados.

- **Serviço de notificações**. O serviço de notificação mantém o usuário informado sobre o status de proteção atual do computador e da operação do Kaspersky Endpoint Security. As notificações podem ser exibidas na tela ou enviadas por e-mail.

- **Kaspersky Security Network**. A participação dos usuários no Kaspersky Security Network oferece maior proteção ao computador mediante a coleta de informações, em tempo real, sobre a reputação de arquivos, os recursos da Web e os programas de computador de usuários no mundo todo.

- **Licença**. A compra de uma licença desbloqueia as funcionalidades completas do aplicativo, fornece acesso às atualizações dos bancos de dados e dos módulos e ao suporte por telefone ou por e-mail em problemas relacionados à instalação, configuração e utilização do aplicativo.

- **Suporte**. Todos os usuários do Kaspersky Endpoint Security podem entrar em contato com os especialistas do Suporte Técnico para obter ajuda. Você pode enviar uma solicitação através da Minha Conta Kaspersky no site do Suporte Técnico ou receber ajuda da equipe do suporte por meio do telefone.

Se o aplicativo devolver um erro ou travar durante a operação, poderá ser reiniciado automaticamente.

Se o aplicativo encontrar erros recorrentes que fazem com que o aplicativo trave, o aplicativo executa as seguintes operações:

1. Desativa as funções de controle e proteção (a funcionalidade de criptografia permanece ativada).

2. Notifica o usuário de que as funções foram desativadas.

3. Tenta restaurar o aplicativo para um estado funcional após atualizar os bancos de dados de antivírus ou aplicar atualizações do módulo do aplicativo.

O aplicativo recebe informações sobre erros recorrentes e o sistema suspende o uso de algoritmos de fins especiais definidos por peritos da Kaspersky.

Requisitos de hardware e software

Para garantir o pleno funcionamento do Kaspersky Endpoint Security, o seu computador deve satisfazer os seguintes requisitos mínimos:

Requisitos gerais mínimos:

- 2 GB de espaço livre no disco rígido
- Processador com uma velocidade de relógio de 1 GHz (que dá suporte ao conjunto de instruções SSE2)
- RAM:
  - 1 GB (para sistemas operacionais de 32 bits)
  - 2 GB (para sistemas operacionais de 64 bits)

Sistemas operacionais compatíveis para computadores pessoais:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 ou posterior;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Education / Enterprise.

Para obter detalhes sobre o suporte do sistema operacional Microsoft Windows 10, consulte a Base de Conhecimento do Suporte Técnico.

Sistemas operacionais para servidores de arquivos com suporte:

- Windows Small Business Server 2008 Standard / Premium (64 bits);
- Windows Small Business Server 2011 Essentials / Standard (64 bits);
- Windows MultiPoint Server 2011 (64 bits);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 ou posterior;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 ou posterior;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Para obter detalhes sobre o suporte dos sistemas operacionais Microsoft Windows Server 2016 e Microsoft Windows Server 2019, consulte a Base de Conhecimento do Suporte Técnico.

Instalar e remover o aplicativo

Esta seção guia você durante a instalação do Kaspersky Endpoint Security em seu computador, a conclusão da configuração inicial, a atualização a partir de uma versão anterior do aplicativo e a desinstalação do aplicativo do computador.

Instalar o aplicativo

Esta seção descreve como instalar o Kaspersky Endpoint Security no computador e realizar a configuração inicial do aplicativo.

Sobre as formas de instalação do aplicativo

O Kaspersky Endpoint Security 10 for Windows pode ser instalado localmente (diretamente no computador do usuário) ou remotamente a partir da estação de trabalho do administrador.

A instalação local do Kaspersky Endpoint Security 10 for Windows pode ser realizada em um dos seguintes modos:

- Em modo interativo usando o Assistente de instalação de aplicativo.

  O modo interativo requer o seu envolvimento no processo de instalação.

- No modo silencioso, por linha de comando.

  Após a instalação ter iniciado no modo silencioso, o seu envolvimento no processo de instalação não é necessário.

O aplicativo pode ser instalado remotamente nos computadores em rede utilizando:

- Conjunto de software do Kaspersky Security Center (consultar o *Guia de Implementação do Kaspersky Security Center*).
- O Editor de Políticas do Grupo do Microsoft Windows (consulte os arquivos de ajuda do sistema operacional).
- System Center Configuration Manager.

Recomendamos fechar todos os aplicativos ativos antes de iniciar a instalação do Kaspersky Endpoint Security (incluindo instalação remota).

Instalar o aplicativo usando o Assistente de Instalação

A interface do aplicativo Assistente de Instalação consiste em uma sequência de janelas que correspondem às etapas de instalação do aplicativo. Você pode navegar nas páginas do Assistente de Instalação usando os botões **Voltar** e **Avançar**. Para fechar o Assistente de Instalação depois de concluir a tarefa, clique no botão **Encerrar**. Para interromper o Assistente de Instalação em qualquer momento, clique no botão **Cancelar**.

Para instalar o aplicativo ou atualizar uma versão anterior usando o Assistente de Instalação:

1. Execute o arquivo setup.exe incluído no kit de distribuição.

   O Assistente de Instalação inicia.

2. Siga as instruções do Assistente de Instalação.

Quando o arquivo setup.exe é iniciado, o Kaspersky Endpoint Security verifica o computador para ver se há algum software incompatível. Por padrão, ao detectar software incompatível, o processo de instalação é interrompido e a lista de aplicativos incompatíveis com o Kaspersky Endpoint Security aparece na tela. Para continuar a instalação, remova esses aplicativos do computador.

Etapa 1. Garantir que o computador atenda aos requisitos de instalação

Antes de instalar o Kaspersky Endpoint Security 10 for Windows em um computador, ou atualizar uma versão anterior do aplicativo, as seguintes condições são verificadas:

- Se o sistema operacional e o service pack atendem aos requisitos de software para instalação de produto.
- Se os requisitos de software foram atendidos.
- Se o usuário tem direitos para instalar o produto de software.

Caso um destes requisitos não seja cumprido, uma notificação é exibida na tela.

Se o computador cumprir os requisitos citados, o Assistente de Instalação busca os aplicativos da Kaspersky que poderiam acarretar conflitos quando executados no mesmo tempo em que o aplicativo é instalado. Caso sejam encontrados tais aplicativos, é solicitado ao usuário que os remova manualmente.

Se os aplicativos detectados incluírem versões anteriores do Kaspersky Endpoint Security, todos os dados que puderem ser migrados (como dados de ativação e configurações do aplicativo) serão conservados e usados durante a instalação do Kaspersky Endpoint Security 10 Service Pack 2 para o Windows, e a versão anterior do aplicativo é automaticamente removida. Isto se aplica às seguintes versões do aplicativo:

- Kaspersky Anti-Virus 6.0 para o Windows Workstations MP4 CF1 / MP4 CF2
- Kaspersky Anti-Virus 6.0 para o Windows Servers MP4 / MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Versão de Manutenção 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Versão de Manutenção 2 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Versão de Manutenção 3 for Windows

Etapa 2. Página de boas-vindas do procedimento de instalação

Se todos os requisitos do aplicativo forem cumpridos, uma página de boas-vindas aparece após a inicialização do pacote de instalação. A página de boas-vindas anuncia o início a instalação no computador do Kaspersky Endpoint Security.

Para continuar com o Assistente de instalação, clique no botão **Avançar**.

Etapa 3. Visualizar o Contrato de Licença

Nesta etapa, o usuário é aconselhado a visualizar o contrato de licença com a Kaspersky.

Leia com atenção o Contrato de Licença e, caso aceite os termos, marque a caixa de seleção **Eu aceito os termos e condições do Contrato de Licença**.

Para regressar à etapa anterior do Assistente de instalação, clique no botão **Voltar**. Para continuar com o Assistente de instalação, clique no botão **Avançar**. Para interromper o Assistente de instalação, clique no botão **Cancelar**.

Etapa 4. Selecionar o tipo de instalação

Nesta etapa, é possível selecionar o tipo mais adequado de instalação do Kaspersky Endpoint Security:

- **Instalação básica**. Se você selecionar este tipo de instalação, os componentes de proteção, Controle de Privilégio de Aplicativo e o Monitoramento de Vulnerabilidades são instalados no computador com as configurações recomendadas por peritos da Kaspersky.
- **Instalação padrão**. Se você selecionar este tipo de instalação, os componentes de proteção e controle com configurações recomendadas pela Kaspersky serão instalados no computador.
- **Instalação Personalizada**. Se você selecionar este tipo da instalação, é instruído a selecionar os componentes para instalar e especificar a pasta de destino do aplicativo.

  Este tipo da instalação permite instalar os componentes que não estão incluídos nas instalações básica e padrão.

A instalação padrão está marcada por padrão.

Para regressar à etapa anterior do Assistente de instalação, clique no botão **Voltar**. Para continuar com o Assistente de instalação, clique no botão **Avançar**. Para interromper o Assistente de instalação, clique no botão **Cancelar**.

Etapa 5. Selecionar componentes do aplicativo a serem instalados

Esta etapa é executada caso você selecione *Instalação personalizada* do aplicativo.

Nesta etapa, é possível selecionar os componentes do Kaspersky Endpoint Security que você pretende instalar. O Antivírus de Arquivos é um componente obrigatório para instalação. Não é possível cancelar a sua instalação.

Por padrão, todos os componentes de aplicativo são selecionados para a instalação exceto os seguintes componentes:

- Prevenção contra ataque BadUSB.
- Criptografia de unidade.
- Criptografia de Arquivo.

- Gerenciador do Microsoft BitLocker.
- Sensor de endpoints da KATA.

O *Gerenciador do Microsoft BitLocker* executa as seguintes funções:

- Gerencia a criptografia de BitLocker construída em sistema operacional Windows.
- Configura as definições da política de criptografia e verifica a sua aplicabilidade para o computador gerenciado.
- Inicia a criptografia e os processos de descriptografia.
- Monitora o status da criptografia no computador gerenciado.
- Armazena centralmente as chaves de recuperação no Servidor de administração do Kaspersky Security Center.

O Sensor de endpoints da KATA é um componente do Kaspersky Anti Targeted Attack Platform. Esta solução é destinada para a detecção rápida de ameaças como ataques visados. O componente monitora continuamente processos, conexões da rede ativas e arquivos que são modificados, e retransmite essas informações a Kaspersky Anti Targeted Attack Platform.

Para selecionar um componente para instalar, clique no ícone ao lado do nome do componente para exibir o menu de contexto e selecione **O recurso será instalado no disco rígido local**. Para obter mais detalhes sobre as tarefas que são executadas pelo componente selecionado e sobre o tamanho em disco necessário para instalá-lo, consulte a parte final da página atual do Assistente de Instalação.

Para visualizar informações detalhadas sobre o espaço disponível nos discos rígidos locais, clique no botão **Volume**. As informações são exibidas na janela **Espaço em disco disponível** que é aberta.

Para cancelar a instalação do componente, selecione a opção **O recurso não estará disponível** no menu de contexto.

Para regressar à lista de componentes instalados por padrão, clique no botão **Redefinir**.

Para regressar à etapa anterior do Assistente de instalação, clique no botão **Voltar**. Para continuar com o Assistente de instalação, clique no botão **Avançar**. Para interromper o Assistente de instalação, clique no botão **Cancelar**.

Etapa 6. Selecionar a pasta de destino

Esta etapa estará disponível se você selecionar a *Instalação personalizada* do aplicativo.

Nesta etapa, você poderá especificar o caminho para a pasta de destino onde será instalado o aplicativo. Para selecionar a pasta de destino do aplicativo, clique no botão **Procurar**.

Para consultar as informações sobre o espaço disponível nos discos rígidos locais, clique no botão **Volume**. As informações aparecem na janela **Requisitos de espaço em disco** exibida.

Para regressar à etapa anterior do Assistente de instalação, clique no botão **Voltar**. Para continuar com o Assistente de instalação, clique no botão **Avançar**. Para interromper o Assistente de instalação, clique no botão **Cancelar**.

Etapa 7. Adicionar exclusões de verificação de vírus

Esta etapa estará disponível se você selecionar a *Instalação personalizada* do aplicativo.

Nesta etapa você pode especificar quais exclusões de verificação de vírus deseja adicionar às configurações do aplicativo.

As caixas de seleção **Excluir áreas que são recomendadas pela Microsoft do escopo da verificação de vírus** / **Excluir áreas recomendadas pela Kaspersky do escopo da verificação de vírus** excluem, respectivamente, as áreas que são recomendadas pela Microsoft ou Kaspersky da zona confiável ou as incluem nesta.

Se for selecionada alguma destas caixas de seleção, o Kaspersky Endpoint Security inclui, respectivamente, as áreas que o Microsoft ou a Kaspersky recomendam na zona confiável. O Kaspersky Endpoint Security não verifica estas áreas para detectar vírus e outras ameaças.

A caixa de seleção **Excluir áreas que são recomendadas pela Microsoft do escopo da verificação de vírus** está disponível quando o Kaspersky Endpoint Security está instalado em um computador que é executado no Microsoft Windows para servidores de arquivo.

Para regressar à etapa anterior do Assistente de instalação, clique no botão **Voltar**. Para continuar com o Assistente de instalação, clique no botão **Avançar**. Para interromper o Assistente de instalação, clique no botão **Cancelar**.

Etapa 8. Preparar a instalação do aplicativo

Recomenda-se proteger o processo de instalação porque o seu computador pode ser infectado com programas maliciosos que podem interferir na instalação do Kaspersky Endpoint Security 10 for Windows.

Por padrão, a proteção do processo de instalação está ativa.

Caso não seja possível instalar o aplicativo (por exemplo, ao efetuar a instalação remota com ajuda do Windows Remote Desktop), é aconselhável desativar a proteção do processo de instalação. Se este é o caso, anule a instalação e inicie o aplicativo Assistente de instalação novamente. Na etapa "Preparar a instalação do aplicativo", desmarque a caixa de seleção **Proteger o processo de instalação**.

A caixa de seleção **Assegurar compatibilidade com Citrix PVS** ativa/desativa a função que instala drivers no modo de compatibilidade do Citrix PVS.

Marque essa caixa de seleção somente se você estiver trabalhando com Citrix Provisioning Services.

A caixa de seleção **Adicionar o caminho para o arquivo avp.com à variável do sistema %PATH%** ativa/desativa a opção que adiciona o caminho para o arquivo avp.com para variável de sistema %PATH%.

Se a caixa de seleção estiver marcada, ao iniciar o Kaspersky Endpoint Security, ou alguma de suas tarefas, da linha de comando, não exige que seja inserido o caminho para o arquivo executável. É suficiente inserir o nome do arquivo executável e o comando para iniciar uma tarefa.

Para regressar à etapa anterior do Assistente de instalação, clique no botão **Voltar**. Para instalar o programa, clique no botão **Instalar**. Para interromper o Assistente de instalação, clique no botão **Cancelar**.

As conexões de rede atuais poderão ser interrompidas durante a instalação do aplicativo no computador. A maior parte das conexões da rede terminadas são restauradas depois que a instalação do aplicativo é concluída.

Etapa 9. Instalação do aplicativo

A instalação do aplicativo poderá demorar algum tempo. Aguarde até que esteja concluída.

Se está atualizando uma versão anterior do aplicativo, esta etapa também inclui a migração e a remoção das configurações da versão anterior do aplicativo.

Depois de terminar a instalação do Kaspersky Endpoint Security, é iniciado o Assistente de Configuração Inicial.

Instalar o aplicativo a partir da linha de comando

O Kaspersky Endpoint Security pode ser instalado a partir da linha de comando em um dos seguintes modos:

- Em modo interativo usando o Assistente de instalação de aplicativo.
- No modo silencioso. Após a instalação ter iniciado no modo silencioso, o seu envolvimento no processo de instalação não é necessário. Para instalar o aplicativo no modo silencioso, use as chaves `/s` e `/qn`.

Para instalar o aplicativo ou atualizar a versão do aplicativo:

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.
2. Vá até a pasta onde o pacote de distribuição do Kaspersky Endpoint Security está localizado.
3. Execute o seguinte comando:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1|0] [/pADDLOCAL=<componente>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<c> /pKLPASSWD=<senha> /pKLPASSWDAREA=<escopo da senha>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<nível de rastreamento>] /s
   ```

   ou

   ```
   msiexec /i <nome do kit de distribuição> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [ALLOWREBOOT=1|0] [ADDLOCAL=<componente>] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<nível de rastreamento> KLPASSWD=<senha> KLPASSWDAREA=<escopo da senha>] [ENABLETRACES=1|0 TRACESLEVEL=<nível de rastreamento>] /qn
   ```

`EULA`	Aceitação ou rejeição dos termos do Contrato de Licença de Usuário Final. Valores disponíveis: • `1` – aceitação dos termos do Contrato de Licença do Usuário Final. • `0` – recusa dos termos do Contrato de Licença do Usuário Final.

	O texto do Contrato de Licença está incluído no kit de distribuição do Kaspersky Endpoint Security. A aceitação dos termos do Contrato de Licença de Usuário Final é necessária para instalar o aplicativo ou para atualizar uma versão do aplicativo.
`PRIVACYPOLICY`	Aceitação ou rejeição da Política de Privacidade. Valores disponíveis: • `1` – aceitação da Política de Privacidade. • `0` – rejeição da Política de Privacidade. O texto da Política de Privacidade está incluído no kit de distribuição do Kaspersky Endpoint Security. Para instalar o aplicativo ou atualizar a versão do aplicativo, aceite a Política de Privacidade.
`KSN`	Acordo ou recusa em participar da Kaspersky Security Network. Se nenhum valor for definido para este parâmetro, o Kaspersky Endpoint Security solicitará a confirmação do seu consentimento ou recusa em participar da KSN quando o Kaspersky Endpoint Security for iniciado pela primeira vez. Valores disponíveis: • `1` – concordo em participar da KSN. • `0` – não aceito participar da KSN (valor padrão). O pacote de distribuição do Kaspersky Endpoint Security é otimizado para uso com a Kaspersky Security Network. Se você optar por não participar da Kaspersky Security Network, atualize o Kaspersky Endpoint Security assim que a instalação for concluída.
`ALLOWREBOOT=1`	Reinício automático do computador, se necessário após a instalação ou atualização do aplicativo. Se nenhum valor for definido para esse parâmetro, a reinicialização automática do computador é bloqueada. Não é necessário reiniciar ao instalar o Kaspersky Endpoint Security. A reinicialização será necessária apenas se você precisar remover aplicativos incompatíveis antes da instalação. A reinicialização também poderá ser necessária quando a versão do aplicativo for atualizada.
`ADDLOCAL`	Selecione componentes adicionais para instalação. Por padrão, todos os componentes de aplicativo são selecionados para a instalação exceto os seguintes componentes: Prevenção contra ataque BadUSB, Criptografia a Nível de Arquivo, Criptografia Completa do Disco, Gerenciamento do BitLocker e Sensor de Endpoints da KATA. Valores disponíveis: • `MSBitLockerFeature`. O componente Gerenciador do Microsoft BitLocker está instalado. • `AntiAPTFeature`. O componente sensor de endpoints da KATA é instalado.
`SKIPPRODUCTCHECK=1`	Desativando a verificação de software incompatível. A lista de softwares incompatíveis está disponível no arquivo incompatible.txt que está incluído no kit de distribuição. Se nenhum valor for definido para esse parâmetro e um software incompatível for detectado, a instalação do Kaspersky Endpoint Security será encerrada.
`SKIPPRODUCTUNINSTALL=1`	Desative a remoção automática de software incompatível detectado. Se nenhum valor for definido para esse parâmetro, o Kaspersky Endpoint Security tentará remover o software incompatível.

KLLOGIN	Defina o nome de usuário para acessar os recursos e configurações do Kaspersky Endpoint Security (o componente Proteção por senha). O nome de usuário é definido junto com as configurações KLPASSWD e KLPASSWDAREA. O nome do usuário padrão é KLAdmin.
KLPASSWD	Especifique uma senha para acessar os recursos e as configurações do Kaspersky Endpoint Security (a senha é especificada em conjunto com os parâmetros de KLLOGIN e KLPASSWDAREA). Se você especificou uma senha mas não especificou um nome de usuário com o parâmetro KLLOGIN, o nome de usuário KLAdmin é usado por padrão.
KLPASSWDAREA	Especifique o escopo da senha para acessar os recursos e as configurações do Kaspersky Endpoint Security. Quando um usuário tenta executar uma ação incluída nesse escopo, o Kaspersky Endpoint Security solicita as credenciais da conta do usuário (parâmetros KLLOGIN e KLPASSWD). Use o caractere ";" para especificar vários valores. Valores disponíveis: • SET – modificar as configurações do aplicativo. • EXIT – sair do aplicativo. • DESPORTEGER – desativar componentes de proteção e interromper tarefas de verificação. • REMOVER POLÍTICA – desativar política do Kaspersky Security Center. • UNINST – remova o aplicativo do computador. • DISCTRL – desativar componentes de controle. • REMOVELIC – remover a chave. • REPORTS – visualizar relatórios.
ENABLETRACES	Ativar ou desativar rastreamentos de aplicativos. Depois que o Kaspersky Endpoint Security inicia, ele salva os arquivos de rastreamento na pasta %ProgramData%/Kaspersky Lab. Valores disponíveis: • 1 – os rastros do aplicativo são ativados. • 0 – os rastros do aplicativo são desativados (valor padrão).
TRACESLEVEL	Nível de detalhe dos rastreamentos. Valores disponíveis: • 100 (crítico). Somente mensagens de erro críticas. • 200 (alto). Mensagens sobre todos os erros, incluindo erros fatais. • 300 (diagnóstico). Mensagens sobre todos os erros e uma seleção de mensagens contendo avisos. • 400 (importante). Todos os avisos e mensagens sobre erros ordinários e críticos e uma seleção de mensagens que contêm informações adicionais.

- `500` (normal). Todos avisos e mensagens sobre erros comuns e críticos; e também mensagens com informações mais detalhadas sobre a operação do aplicativo em modo normal (valor padrão).
- `600` (baixo). Todas as mensagens possíveis.

Exemplo:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Após a instalação do aplicativo, o Kaspersky Endpoint Security ativa a licença de avaliação, a menos que você indicou um código de ativação no arquivo setup.ini. Uma licença de avaliação geralmente tem um termo curto. Quando a licença de avaliação expira, todos os recursos do aplicativo do Kaspersky Endpoint Security são desativados. Para continuar a usar o aplicativo, é necessário ativar uma licença comercial.

Ao instalar o aplicativo ou ao fazer um upgrade da versão do aplicativo no modo silencioso, o uso dos seguintes arquivos é suportado:

- setup.ini – definições gerais de configuração do aplicativo;
- install.cfg – configurações locais do Kaspersky Endpoint Security;
- setup.reg – chaves do registro.

  As chaves de registro do arquivo setup.reg serão gravadas no registro apenas se o valor `setup.reg` estiver definido para o parâmetro `SetupReg` no arquivo setup.ini. O arquivo setup.reg é gerado pelos especialistas da Kaspersky. Não é recomendado modificar os conteúdos desse arquivo.

Para aplicar configurações dos arquivos setup.ini, install.cfg e setup.reg, coloque esses arquivos na pasta que contém o pacote de distribuição do Kaspersky Endpoint Security.

Instalar remotamente o aplicativo usando o System Center Configuration Manager

Estas instruções aplicam-se ao System Center Configuration Manager 2012 R2.

Para instalar remotamente um aplicativo usando o System Center Configuration Manager:

1. Abra o console do Configuration Manager.
2. Na parte direita do console, na seção **Gerenciamento de aplicativos**, selecione **Pacotes**.
3. Na parte superior do console, no painel de comando, clique no botão **Criar pacote**.

Isto inicia o *Novo Assistente de Aplicativos e Pacotes*.

4. No Novo Assistente de Aplicativos e Pacotes:

   a. Na seção **Pacote**:

   - No campo **Nome**, insira o nome do pacote de instalação.
   - No campo **Pasta de origem**, especifique o caminho para a pasta que contém o kit de distribuição do Kaspersky Endpoint Security.

   b. Na seção **Tipo de aplicativo**, selecione a opção **Aplicativo padrão**.

   c. Na seção **Aplicativo padrão**:

   - No campo **Nome**, digite o nome exclusivo do pacote de instalação (por exemplo, o nome do aplicativo inclusive a versão).
   - No campo **Linha de comando**, especifique as opções de instalação do Kaspersky Endpoint Security na linha de comando.
   - Clique no botão **Procurar** para especificar o caminho para o arquivo executável do aplicativo.
   - Certifique-se de que a lista **Modo de execução** tenha o item **Executar com direitos de administrador** selecionado.

   d. Na seção **Requisitos**:

   - Marque a caixa de seleção **Iniciar outro aplicativo primeiro** se desejar que um aplicativo diferente seja iniciado antes de instalar o Kaspersky Endpoint Security.

     Selecione o aplicativo na lista suspensa **Aplicativo** ou especifique o caminho para o arquivo executável desse aplicativo clicando no botão **Procurar**.

   - Selecione a opção **Este aplicativo pode ser iniciado somente nas plataformas especificadas** na seção **Requisitos da plataforma** se você quiser que o aplicativo seja instalado somente nos sistemas operacionais especificados.

     Na lista abaixo, selecione as caixas em frente dos sistemas operacionais nos quais o Kaspersky Endpoint Security será instalado.

   Esta etapa é opcional.

   e. Na seção **Resumo**, verifique todos os valores inseridos das configurações e clique **em Avançar**.

   O pacote de instalação criado aparecerá na seção **Pacotes** na lista de pacotes de instalação disponíveis.

5. No menu de contexto do pacote de instalação, selecione **Implementar**.

   Isto inicia o *Assistente de Implementação*.

6. No Assistente de Implementação:

   a. Na seção **Geral**:

   - No campo **Software**, digite o nome exclusivo do pacote de instalação ou selecione o pacote de instalação na lista clicando no botão **Procurar**.

- No campo **Coleção**, digite o nome da coleção de computadores nos quais o aplicativo será instalado ou selecione a coleção clicando no botão **Procurar**.

b. Na seção **Contém**, adicione pontos de distribuição (para a informação mais detalhada, consulte a documentação de ajuda do System Center Configuration Manager).

c. Se necessário, especifique os valores das outras configurações no Assistente de Implementação. Estas configurações são opcionais para a instalação remota do Kaspersky Endpoint Security.

d. Na seção **Resumo**, verifique todos os valores inseridos das configurações e clique **em Avançar**.

Depois que o Assistente de Implementação for concluído, uma tarefa será criada para a instalação remota do Kaspersky Endpoint Security.

Descrição das configurações de instalação do arquivo setup.ini

O arquivo setup.ini é usado durante a instalação do aplicativo através da linha de comando ou do Editor de Política de Grupo do Microsoft Windows. Para aplicar as configurações do arquivo setup.ini, coloque esse arquivo na pasta que contém o pacote de distribuição do Kaspersky Endpoint Security.

O arquivo setup.ini consiste nas seguintes seções:

- `[Instalação]` – opções gerais de instalação do aplicativo.
- `[Componentes]` – seleção dos componentes do aplicativo a ser instalados. Se nenhum dos componentes for especificado, todos os componentes que estão disponíveis para o sistema operacional são instalados. O Antivírus de Arquivos é um componente obrigatório e é instalado no computador independentemente das configurações indicadas nesta seção.
- `[Tarefas]` – seleção de tarefas a serem incluídas na lista de tarefas do Kaspersky Endpoint Security. Se nenhuma tarefa for especificada, todas as tarefas serão incluídas na lista de tarefas do Kaspersky Endpoint Security.

Em alternativa ao valor `1`, é possível usar os valores `sim`, `ligado`, `ativar` e `ativado`.

Em alternativa ao valor `0`, é possível usar os valores `não`, `desligado`, `desativar` e `desativado`.

Configurações do arquivo setup.ini

Seção	Parâmetro	Descrição
`[Configuração]`	`InstallDir`	Caminho até a pasta de instalação do aplicativo.
	`ActivationCode`	Código de ativação do Kaspersky Endpoint Security.
	`Eula`	Aceitação ou rejeição dos termos do Contrato de Licença de Usuário Final. Valores disponíveis: • `1` – aceitação dos termos do Contrato de Licença do Usuário Final. • `0` – recusa dos termos do Contrato de Licença do Usuário Final.

		O texto do Contrato de Licença está incluído no kit de distribuição do Kaspersky Endpoint Security. A aceitação dos termos do Contrato de Licença de Usuário Final é necessária para instalar o aplicativo ou para atualizar uma versão do aplicativo.
	`PrivacyPolicy`	Aceitação ou rejeição da Política de Privacidade. Valores disponíveis: • `1` – aceitação da Política de Privacidade. • `0` – rejeição da Política de Privacidade. O texto da Política de Privacidade está incluído no kit de distribuição do Kaspersky Endpoint Security. Para instalar o aplicativo ou atualizar a versão do aplicativo, aceite a Política de Privacidade.
	`KSN`	Acordo ou recusa em participar da Kaspersky Security Network. Se nenhum valor for definido para este parâmetro, o Kaspersky Endpoint Security solicitará a confirmação do seu consentimento ou recusa em participar da KSN quando o Kaspersky Endpoint Security for iniciado pela primeira vez. Valores disponíveis: • `1` – concordo em participar da KSN. • `0` – não aceito participar da KSN (valor padrão). O pacote de distribuição do Kaspersky Endpoint Security é otimizado para uso com a Kaspersky Security Network. Se você optar por não participar da Kaspersky Security Network, atualize o Kaspersky Endpoint Security assim que a instalação for concluída.
	`Login`	Defina o nome de usuário para acessar os recursos e configurações do Kaspersky Endpoint Security (o componente Proteção por senha). O nome de usuário é definido junto com as configurações `Password` e `PasswordArea`. O nome do usuário padrão é KLAdmin.
	`Senha`	Especifique uma senha para acessar os recursos e as configurações do Kaspersky Endpoint Security (a senha é especificada em conjunto com os parâmetros de `Login` e `PasswordArea`). Se você especificou uma senha mas não especificou um nome de usuário com o parâmetro `Login`, o nome de usuário KLAdmin é usado por padrão.
	`PasswordArea`	Especifique o escopo da senha para acessar os recursos e as configurações do Kaspersky Endpoint Security. Quando um usuário tenta executar uma ação incluída nesse escopo, o

		Kaspersky Endpoint Security solicita as credenciais da conta do usuário (parâmetros `Login` e `Senha`). Use o caractere "`;`" para especificar vários valores. Valores disponíveis: • `SET` – modificar as configurações do aplicativo. • `EXIT` – sair do aplicativo. • `DESPORTEGER` – desativar componentes de proteção e interromper tarefas de verificação. • `REMOVER POLÍTICA` – desativar política do Kaspersky Security Center. • `UNINST` – remova o aplicativo do computador. • `DISCTRL` – desativar componentes de controle. • `REMOVELIC` – remover a chave. • `REPORTS` – visualizar relatórios.
	`SelfProtection`	Ativar ou desativar o mecanismo de proteção da instalação do aplicativo. Valores disponíveis: • `1` – o mecanismo de proteção da instalação do aplicativo é ativado. • `0` – o mecanismo de proteção da instalação do aplicativo é desativado. Você pode desativar a proteção de instalação. A proteção da instalação inclui proteção contra a falsificação do pacote de distribuição por programas maliciosos, bloqueio do acesso à pasta de instalação do Kaspersky Endpoint Security e bloqueio do acesso à hive do registro do sistema que contém as chaves do aplicativo. Caso não seja possível instalar o aplicativo (por exemplo, ao efetuar a instalação remota com ajuda do Windows Remote Desktop), é aconselhável desativar a proteção do processo de instalação.
	`Reboot=1`	Reinício automático do computador, se necessário após a instalação ou atualização do aplicativo. Se nenhum valor for definido para esse parâmetro, a reinicialização automática do computador é bloqueada. Não é necessário reiniciar ao instalar o Kaspersky Endpoint Security. A reinicialização será necessária apenas se você precisar remover aplicativos incompatíveis antes da instalação. A reinicialização também poderá ser necessária quando a versão do aplicativo for atualizada.

	`AddEnvironment`	Complemente a variável de sistema %PATH% com o caminho para arquivos executáveis localizados na pasta de configuração do Kaspersky Endpoint Security. Valores disponíveis: • `1` – a variável de sistema %PATH% é complementada com o caminho para os arquivos executáveis localizados na pasta de configuração do Kaspersky Endpoint Security. • `0` – a variável de sistema %PATH% não é complementada com o caminho para arquivos executáveis localizados na pasta de configuração do Kaspersky Endpoint Security.
	`AMPPL`	Ative ou desative a proteção do serviço Kaspersky Endpoint Security usando a tecnologia AM-PPL (Antimalware Protected Process Light). Valores disponíveis: • `1` – a proteção do serviço Kaspersky Endpoint Security usando a tecnologia AM-PPL é ativada. • `0` – a proteção do serviço Kaspersky Endpoint Security usando a tecnologia AM-PPL é desativada.
	`SetupReg`	Ativa a gravação das chaves do registro do arquivo setup.reg para o registro. Valor do parâmetro `SetupReg: setup.reg`.
	`EnableTraces`	Ativar ou desativar rastreamentos de instalação do aplicativo. O Kaspersky Endpoint Security salva os arquivos de rastreamento na pasta %ProgramData%/Kaspersky Lab. Valores disponíveis: • `1` – os rastreamentos de instalação do aplicativo estão ativados. • `0` – os rastreamentos de instalação do aplicativo estão desativados (valor padrão).
	`TracesLevel`	Nível de detalhe dos rastreamentos. Valores disponíveis: • `100` (crítico). Somente mensagens de erro críticas. • `200` (alto). Mensagens sobre todos os erros, incluindo erros fatais. • `300` (diagnóstico). Mensagens sobre todos os erros e uma seleção de mensagens contendo avisos. • `400` (importante). Todos os avisos e mensagens sobre erros ordinários e críticos e

		uma seleção de mensagens que contêm informações adicionais. • `500` (normal). Todos avisos e mensagens sobre erros comuns e críticos; e também mensagens com informações mais detalhadas sobre a operação do aplicativo em modo normal (valor padrão). • `600` (baixo). Todas as mensagens possíveis.
`[Componentes]`	`ALL`	Instale todos os componentes. Se o valor de parâmetro `1` for especificado, todos os componentes serão instalados apesar das configurações de instalação de componentes individuais.
	`MailAntiVirus`	Antivírus de e-mail.
	`IMAntiVirus`	Antivírus de mensagem instantânea.
	`WebAntiVirus`	Antivírus da internet.
	`ApplicationPrivilegeControl`	Controle de privilégios do aplicativo.
	`SystemWatcher`	Inspetor do sistema.
	`Firewall`	Firewall.
	`NetworkAttackBlocker`	Bloqueio de Ataque de Rede.
	`WebControl`	Controle da Web.
	`DeviceControl`	Controle de Dispositivo.
	`ApplicationStartupControl`	Controle de Inicialização de Aplicativo.
	`FileEncryption`	Bibliotecas de Criptografia a Nível de Arquivo.
	`DiskEncryption`	Bibliotecas de Criptografia Completa do Disco.
	`VulnerabilityAssessment`	Monitoramento de Vulnerabilidades.
	`KeyboardAuthorization`	Prevenção contra ataque BadUSB.
	`AntiAPT`	Sensor de endpoints da KATA
	`MSBitLocker`	Gerenciador do Microsoft BitLocker.
	`AdminKitConnector`	Conector do Agente de Rede para a administração remota do aplicativo através do Kaspersky Security Center. Valores disponíveis: • `1` – o Conector do Agente de Rede é instalado. • `0` – o Conector do Agente de Rede não é instalado.
`[Tarefas]`	`ScanMyComputer`	Tarefa de Verificação Completa. Valores disponíveis: • `1` – a tarefa está incluída na lista de tarefas do Kaspersky Endpoint Security.

		• `0` – a tarefa não está incluída na lista de tarefas do Kaspersky Endpoint Security.
	`ScanCritical`	Tarefa de Verificação de Áreas Críticas. Valores disponíveis: • `1` – a tarefa está incluída na lista de tarefas do Kaspersky Endpoint Security. • `0` – a tarefa não está incluída na lista de tarefas do Kaspersky Endpoint Security.
	`Updater`	Tarefa de atualização. Valores disponíveis: • `1` – a tarefa está incluída na lista de tarefas do Kaspersky Endpoint Security. • `0` – a tarefa não está incluída na lista de tarefas do Kaspersky Endpoint Security.

Assistente de Configuração Inicial

O Assistente de Configuração Inicial do Kaspersky Endpoint Security é iniciado no final do procedimento de configuração do aplicativo. O Assistente de Configuração Inicial permite ativar o aplicativo e recolhe informações sobre os aplicativos incluídos no sistema operacional. Esses aplicativos são adicionados à lista de aplicativos confiáveis, cujas ações dentro do sistema operacional não estão sujeitas a nenhuma restrição.

A interface do Assistente de Configuração Inicial é constituída por uma sequência de páginas (etapas). É possível navegar nas janelas do Assistente de Configuração Inicial através dos botões **Voltar** e **Avançar**. Para concluir o procedimento do Assistente de Configuração Inicial, clique no botão **Encerrar**. Para interromper o procedimento do Assistente de Configuração Inicial em qualquer etapa, clique em **Cancelar**.

Se o Assistente de Configuração Inicial for interrompido por algum motivo, as configurações já especificadas não serão salvas. Na próxima tentativa de utilização do aplicativo, o Assistente de Configuração Inicial será iniciado novamente e você terá que definir as configurações a partir do zero.

Ativar o aplicativo

O aplicativo deve ser ativado em um computador com a data e hora do sistema atuais. Se a data e hora do sistema forem alteradas após a ativação do aplicativo, a chave fica inoperacional. O aplicativo muda para um modo de operação sem atualizações e o Kaspersky Security Network não está disponível. A chave pode ser tornada novamente operacional somente reinstalando o sistema operacional.

Nesta etapa, selecione uma das seguintes opções de ativação do Kaspersky Endpoint Security:

- **Ativar com um código de ativação**. Para ativar o aplicativo com um código de ativação, selecione esta opção e insira um código de ativação.
- **Ativar com arquivo de chave**. Selecione esta opção para ativar o aplicativo com um arquivo de chave.

- **Ativar a versão de avaliação**. Selecione esta opção para ativar a versão de avaliação do aplicativo. O usuário pode utilizar a versão totalmente funcional do aplicativo durante o prazo limitado pela licença da versão de avaliação do aplicativo. Após a expiração da licença, o funcionamento do aplicativo é bloqueado e não é possível ativar novamente a versão de avaliação.

- **Ativar mais tarde**. Selecione esta opção para ignorar a etapa de ativação do Kaspersky Endpoint Security. O usuário conseguirá usar somente os componentes Antivírus de Arquivos e Firewall. O usuário conseguirá atualizar os bancos de dados de antivírus e módulos do Kaspersky Endpoint Security uma única vez após a instalação. A opção **Ativar mais tarde** só está disponível na primeira vez que o Assistente de Configuração Inicial é usado, imediatamente após a instalação do aplicativo.

É necessário conexão à Internet para ativar a versão de avaliação do aplicativo ou para ativar o aplicativo com um código de ativação.

Para prosseguir com as etapas seguintes do Assistente de Configuração Inicial, selecione uma opção de ativação e clique no botão **Seguinte**. Para interromper o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Ativar com um código de ativação

Esta etapa só está disponível quando você ativa o aplicativo com um código de ativação. Esta etapa é ignorada ao ativar a versão de avaliação do aplicativo ou ao ativar o aplicativo com um arquivo de chave.

Nesta etapa, o Kaspersky Endpoint Security envia dados para o servidor de ativação, para verificar o código de ativação inserido:

- Se a verificação do código de ativação tiver êxito, o Assistente de Configuração Inicial avançará automaticamente para a próxima janela.

- Se a verificação do código de ativação falhar, a mensagem correspondente será exibida. Neste caso, você deverá entrar em contato com o fornecedor de software com quem adquiriu a licença do Kaspersky Endpoint Security.

- Se o número de ativações com o código de ativação for excedido, a notificação correspondente será exibida. O Assistente de Configuração Inicial é interrompido e o aplicativo sugere que entre em contato com o Suporte Técnico da Kaspersky.

Para regressar à etapa anterior do Assistente de Configuração Inicial, clique no botão **Voltar**. Para interromper o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Ativar com um arquivo de chave

Esta etapa só está disponível quando você ativa o aplicativo com um arquivo de chave.

Nesta etapa, especifique o caminho para o arquivo de chave. Para isso, clique no botão **Procurar** e selecione um arquivo de chave no formulário `<ID do arquivo>.key`.

Após selecionar o arquivo de chave, serão exibidas as seguintes informações na parte inferior da janela:

- Chave
- Tipo de licença (comercial ou de teste) e o número de computadores abrangidos pela licença
- Data da ativação do aplicativo no computador
- Data de validade da licença
- Funcionalidade do aplicativo disponível nos termos da licença
- Notificações sobre problemas com a chave, caso haja. Por exemplo, a *Lista negra de chaves corrompidas*.

Para regressar à etapa anterior do Assistente de Configuração Inicial, clique no botão **Voltar**. Para avançar com o Assistente de Configuração Inicial, clique no botão **Avançar**. Para interromper o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Selecionar as funções a serem ativadas

Esta etapa só está disponível quando você ativa a versão de avaliação do aplicativo.

Nesta etapa, você pode selecionar a funcionalidade que ficará disponível depois da ativação do aplicativo:

- **Instalação básica**. Se essa opção for selecionada, somente os componentes de proteção, o Controle de Privilégios de Aplicativo e o Monitoramento de Vulnerabilidades estarão disponíveis após a ativação do aplicativo.
- **Instalação padrão**. Se esta opção estiver selecionada, apenas componentes de proteção e controle do aplicativo estarão disponíveis após a ativação.
- **Instalação completa**. Se esta opção for selecionada, todos os componentes instalados, incluindo a funcionalidade de criptografia de dados, estarão disponíveis após a ativação do aplicativo.

Se você tiver selecionado mais componentes do que as licenças adquiridas durante a instalação, depois da ativação do aplicativo, os componentes que estão indisponíveis sob a licença serão instalados mas não estarão operacionais. Se a licença comprada permitir o uso de mais componentes do que os atualmente instalados, após o aplicativo ser ativado, os componentes que não foram instalados serão listados na seção **Licenciamento**.

A instalação padrão está marcada por padrão.

Para regressar à etapa anterior do Assistente de Configuração Inicial, clique no botão **Voltar**. Para avançar com o Assistente de Configuração Inicial, clique no botão **Avançar**. Para interromper o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Concluir a ativação

Nesta etapa, o Assistente de Configuração Inicial informa sobre a ativação bem-sucedida do Kaspersky Endpoint Security. São fornecidas as seguintes informações sobre a licença:

- Tipo de licença (comercial ou de teste) e o número de computadores abrangidos pela licença
- Data de validade da licença
- Funcionalidade do aplicativo disponível nos termos da licença

Para avançar com o Assistente de Configuração Inicial, clique no botão **Avançar**. Para interromper o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Analisar o sistema operacional

Nesta etapa, são coletadas informações sobre os aplicativos que estão incluídos no sistema operacional. Esses aplicativos são adicionados à lista de aplicativos confiáveis, cujas ações dentro do sistema operacional não estão sujeitas a nenhuma restrição.

Os restantes aplicativos são analisados após serem iniciados pela primeira vez após a instalação do Kaspersky Endpoint Security.

Para interromper o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Concluir a configuração inicial do aplicativo

A janela do Assistente de Configuração Inicial contém informações sobre a conclusão do processo de instalação do Kaspersky Endpoint Security.

Se você pretender iniciar o Kaspersky Endpoint Security, clique no botão **Concluir**.

Se você pretender sair do Assistente de Configuração Inicial sem iniciar o Kaspersky Endpoint Security, desmarque a caixa de seleção **Iniciar o Kaspersky Endpoint Security 10 for Windows** e clique em **Concluir**.

Declaração do Kaspersky Security Network

Nesta etapa, você é convidado a participar no Kaspersky Security Network.

Consulte a Declaração do Kaspersky Security Network:

- Se você aceitar todos dos seus termos, selecione a opção **Eu aceito os termos da participação no Kaspersky Security Network** na janela do Assistente de Configuração Inicial.
- Se você não aceitar os termos da participação no Kaspersky Security Network, selecione a opção **Eu não aceito os termos da participação no Kaspersky Security Network** na janela do Assistente de Configuração Inicial.

Para continuar com o Assistente de Configuração Inicial, clique em **OK**.

Sobre as formas de atualização de uma versão antiga do aplicativo

Para atualizar uma versão anterior do aplicativo para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, descriptografe todos os discos rígidos criptografados.

É possível atualizar os seguintes aplicativos para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 (compilação 6.0.4.1424)/MP4 CF2 (compilação 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (compilação 6.0.4.1424)/MP4 CF2 (compilação 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (compilação 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (compilação 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (compilação 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (compilação 10.2.5.3201).

Quando um dos aplicativos listados anteriormente é atualizado para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, os conteúdos da Quarentena e Backup não são transferidos.

É possível atualizar a versão antiga do aplicativo da seguinte forma:

- Localmente, no modo interativo, usando o Assistente de instalação de aplicativo.
- Localmente, no modo não interativo, a partir da linha de comando
- Remotamente, com o conjunto de software do Kaspersky Security Center (consulte o *Guia de Implementação do Kaspersky Security Center*)
- Remotamente através do Editor de Políticas do Grupo do Microsoft Windows (consulte os arquivos de ajuda do sistema operacional)

Ao atualizar uma versão anterior do aplicativo para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, não é necessário remover a versão anterior do aplicativo. É recomendável fechar todos os aplicativos ativos antes de iniciar a atualização do aplicativo.

Remover o aplicativo

Esta seção descreve como remover o Kaspersky Endpoint Security do computador.

Sobre os meios de remoção do aplicativo

A remoção do Kaspersky Endpoint Security deixará o computador e os dados do usuário sem proteção contra ameaças.

Kaspersky Endpoint Security pode ser removido do computador de vários modos:

- Localmente, no modo interativo, usando o Assistente de instalação
- Localmente, no modo não interativo, a partir da linha de comando
- Remotamente, com o conjunto de software do Kaspersky Security Center (consulte o *Guia de Implementação do Kaspersky Security Center* para mais detalhes)
- Remotamente através do Editor de Políticas do Grupo do Microsoft Windows (consulte os arquivos de ajuda do sistema operacional)

Remover o aplicativo por meio do Assistente de Instalação

Para remover o Kaspersky Endpoint Security usando o Assistente de Instalação:

1. No menu **Iniciar**, selecione **Aplicativos** → **Kaspersky Endpoint Security 10 for Windows** → **Modificar, Reparar ou Remover**.

   O Assistente de Instalação inicia.

2. Na janela **Modificar, Reparar ou Remover o aplicativo** do Assistente de Instalação, clique no botão **Remover**.

3. Siga as instruções do Assistente de Instalação.

Etapa 1. Salvar dados do aplicativo para uso futuro

Nesta etapa, você pode especificar quais dos dados usados pelo aplicativo você quer guardar para uso durante a instalação seguinte do aplicativo (por exemplo, instalar uma versão posterior). Se você não especificar nenhum dado, o aplicativo será completamente removido.

Para salvar os dados do aplicativo para uso futuro,

marque as caixas de seleção perto dos tipos de dados que você pretende salvar:

- **Dados de ativação** – dados que eliminam a necessidade de ativar o aplicativo que você instalar no futuro. O aplicativo é automaticamente ativado sob a licença atual, desde que a licença não tenha expirado no momento da instalação.
- **Arquivos de Backup e Quarentena** – arquivos que são verificados pelo aplicativo e colocados em Backup ou Quarentena.

  Os arquivos de Backup e Quarentena que são salvos após a remoção do aplicativo podem ser acessados somente com a mesma versão do aplicativo usada para salvar esses arquivos.

  Se desejar usar objetos de Backup e Quarentena depois de remover o aplicativo, será necessário restaurar estes objetos nos respectivos armazenamentos antes da remoção do aplicativo. Contudo, os especialistas da Kaspersky não recomendam restaurar arquivos do Backup e Quarentena, pois isso poderá danificar o computador.

- **Configurações de operação do aplicativo** – valores das configurações do aplicativo que são selecionados durante a configuração.

- **Armazenamento local das chaves de criptografia** – dados que fornecem acesso direto a arquivos e dispositivos que foram criptografados antes da remoção do aplicativo. Os arquivos e unidades criptografados podem ser acessados diretamente após a reinstalação do aplicativo com a funcionalidade de criptografia.

  Esta caixa de seleção está selecionada por padrão.

Para continuar com o Assistente de instalação, clique no botão **Avançar**. Para interromper o Assistente de instalação, clique no botão **Cancelar**.

Etapa 2. Confirmar a remoção do aplicativo

Uma vez que a remoção do aplicativo coloca em risco a segurança do computador, é solicitada a confirmação de que você pretende remover o aplicativo. Para fazê-lo, clique no botão **Remover**.

Para interromper a remoção do aplicativo em qualquer momento, você pode cancelar esta operação clicando no botão **Cancelar**.

Etapa 3. Remover o aplicativo. Concluir a remoção

Nesta etapa, o Assistente de Instalação remove o aplicativo do computador. Aguarde até que a remoção do aplicativo esteja concluída.

Ao remover o aplicativo, poderá ser necessário reiniciar o sistema operacional. Se você decidir não reiniciar de imediato, a conclusão do procedimento de remoção do aplicativo é adiada até que o sistema operacional seja reiniciado ou até que o computador seja desligado e ligado novamente.

Remover o aplicativo a partir da linha de comando

É possível iniciar o processo de desinstalação do aplicativo a partir da linha de comando. A desinstalação é realizada no modo interativo ou silencioso (sem iniciar o Assistente de Instalação do Aplicativo).

Para iniciar o processo de desinstalação do aplicativo no modo interativo,

na linha de comando, digite `setup.exe /x` ou `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

O Assistente de Instalação inicia. Siga as instruções do Assistente de Instalação.

Para iniciar o processo de desinstalação do aplicativo no modo silencioso,

na linha de comando, digite `setup.exe /s /x` ou `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

Isso inicia o processo de desinstalação de aplicativo no modo silencioso (sem iniciar o Assistente de instalação).

Se a operação de desinstalação do aplicativo for protegida por senha, o nome de usuário e a senha correspondentes devem ser inseridos na linha de comando.

Para remover o aplicativo da linha de comando no modo interativo quando o nome e a senha de usuário para autenticação de remoção, modificação ou reparação do Kaspersky Endpoint Security estiverem definidos,

Na linha de comando, digite `setup.exe /pKLLOGIN=<Nome de usuário> /pKLPASSWD=***** /x` ou

```
msiexec.exe KLLOGIN=<Nome de usuário> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-
56E6EF762275}.
```

O Assistente de Instalação inicia. Siga as instruções do Assistente de Instalação.

Para remover o aplicativo da linha de comando no modo silencioso quando o nome e a senha de usuário para autenticação de remoção, modificação ou reparação do Kaspersky Endpoint Security estiverem definidos:

Na linha de comando, digite `setup.exe /pKLLOGIN=<Nome de usuário> /pKLPASSWD=***** /s /x` ou

```
msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<Nome de usuário>
KLPASSWD=***** /qn.
```

Remover objetos e dados que permanecem após a operação de teste do Agente de Autenticação

Durante a desinstalação de aplicativo, se o Kaspersky Endpoint Security detectar objetos e dados que permaneceram no disco rígido de sistema depois da operação de teste do Agente de Autenticação, a desinstalação do aplicativo é interrompida e fica impossível até que esses objetos e dados sejam removidos.

Os objetos e dados podem permanecer no disco rígido do sistema após a operação de teste do Agente de Autenticação, somente em casos excecionais. Por exemplo, isso pode acontecer se o computador não tiver sido reiniciado após ser aplicada uma política do Kaspersky Security Center com configurações de criptografia, ou se o aplicativo falhar ao ser iniciado após a operação de teste do Agente de Autenticação.

É possível remover objetos e dados que permanecem no disco rígido do sistema pós a operação de teste do Agente de Autenticação de duas formas:

- Desativando a política do Kaspersky Security Center.
- Usando o Utilitário de Restauração.

Para usar uma política do Kaspersky Security Center para remover objetos e dados que permaneceram depois da operação de teste do Agente de Autenticação:

1. Aplique no computador uma política do Kaspersky Security Center com configurações definidas para decriptografar todos os discos rígidos de computador.
2. Inicie o Kaspersky Endpoint Security.

Para usar o Utilitário de Restauração para remover objetos e dados que permanecem depois da operação de teste do Agente de Autenticação:

1. Inicie o Utilitário de Restauração executando o arquivo executável fdert.exe criado usando o Kaspersky Endpoint Security no computador com o disco rígido do sistema conectado nos quais permaneceram os objetos e dados depois da operação de teste do Agente de Autenticação.

2. Na lista suspensa **Selecionar dispositivo**, na janela Utilitário de Restauração, selecione o disco rígido do sistema que contém os objetos e dados a remover.

3. Clique no botão **Verificar**.

4. Clique no botão **Excluir objetos e dados AA**.

   Isso inicia o processo de remoção de objetos e dados que permaneceram após a operação de teste do Agente de Autenticação.

Após remover os objetos e dados que permaneceram após a operação de teste do Agente de Autenticação, poderá ser necessário remover as informações sobre a incompatibilidade do aplicativo com o Agente de Autenticação.

Para remover informações sobre a incompatibilidade do aplicativo com o Agente de Autenticação,

insira o comando `avp pbatestreset` na linha de comando.

Os componentes de criptografia devem estar instalados para que o comando `avp pbatestreset` seja executado.

Interface do aplicativo

Esta seção descreve os principais elementos da interface do aplicativo.

Ícone do aplicativo na área de notificação da barra de tarefas

Logo após a instalação do Kaspersky Endpoint Security, o ícone do aplicativo aparece na área de notificação da barra de tarefas do Microsoft Windows.

O ícone atende às seguintes finalidades:

- Indicar a atividade do aplicativo.
- Funcionar como um atalho para o menu de contexto e para a janela principal do aplicativo.

Indicação da atividade do aplicativo

O ícone do aplicativo funciona como indicador da atividade do aplicativo:

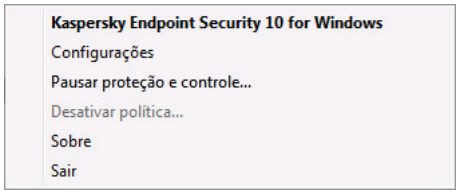
- O ícone indica que todos os componentes de proteção do aplicativo estão ativos.
- O ícone indica que eventos importantes, e que requerem ação, ocorreram na operação do Kaspersky Endpoint Security. Por exemplo, o Antivírus de Arquivos está desativado ou os bancos de dados estão desatualizados.
- O ícone indica que ocorreram eventos críticos na operação do Kaspersky Endpoint Security. Por exemplo, falha na operação de um componente ou corrupção dos bancos de dados do aplicativo.

Menu de contexto do ícone do aplicativo

O menu de contexto do ícone do aplicativo contém os seguintes itens:

- **Kaspersky Endpoint Security 10 for Windows**. Abre a guia **Proteção e Controle** da janela principal do aplicativo. A guia **Proteção e Controle** permite ajustar o funcionamento dos componentes e das tarefas do aplicativo e exibir estatísticas de arquivos processados e ameaças detectadas.
- **Configurações**. Abre a guia **Configurações** na janela principal do aplicativo. A guia **Configurações** permite editar as configurações padrão do aplicativo.
- **Pausar proteção e controle** / **Continuar a proteção e controle**. Pausa / Continua a operação dos componentes de proteção e controle. Este item do menu de contexto não afeta a tarefa de atualização e de verificação, estando disponível apenas quando a política do Kaspersky Security Center está desativada.
- **Desativar política** / **Ativar política**. Desativa / Ativa a política do Kaspersky Security Center. Este item do menu de contexto está disponível quando o Kaspersky Endpoint Security é executado com base em uma política e quando houver uma senha definida para desativar a política do Kaspersky Security Center.
- **Sobre**. Este item abre uma janela de informações que contém detalhes do aplicativo.

- **Sair**. Este item encerra o Kaspersky Endpoint Security. Quando você clica neste menu de contexto o aplicativo é retirado da RAM do computador.



Menu de contexto do ícone do aplicativo

Você pode abrir o menu de contexto do ícone do aplicativo ao posicionar o mouse no ícone do aplicativo, na área de notificação da barra de tarefas do Microsoft Windows, e clicar com o botão direito.

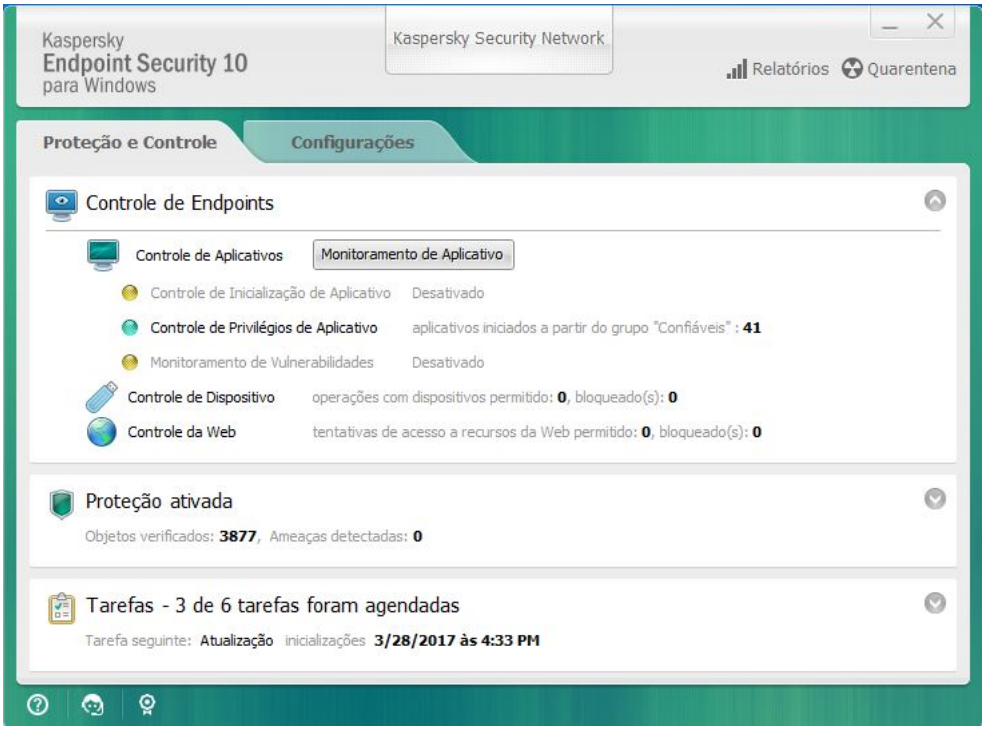
Janela principal do aplicativo

A janela principal do Kaspersky Endpoint Security contém elementos da interface que permitem o acesso às principais funções do aplicativo.

A janela principal do aplicativo é dividida em quatro partes (veja a figura abaixo):

- No canto superior da janela estão elementos da interface que permitem a exibição das seguintes informações:
  - Detalhes do aplicativo
  - Estatísticas do Kaspersky Security Network
  - Lista de arquivos não processados
  - Lista de vulnerabilidades detectadas
  - Lista de arquivos em quarentena
  - Armazenamento de cópias de arquivos infectados excluídos pelo aplicativo
  - Relatórios sobre eventos ocorridos durante a execução do aplicativo, ou durante o desempenho de tarefas, em todos ou em alguns componentes do aplicativo
- A guia **Proteção e Controle** permite ajustar o funcionamento dos componentes do aplicativo e a conclusão das tarefas. A guia **Proteção e Controle** é exibida quando a janela principal do aplicativo é aberta.
- A guia **Configurações** permite editar as configurações padrão do aplicativo.
- A parte inferior da janela contém os seguintes elementos:
  - **Botão**. Ao clicar neste botão, você será direcionado para o sistema de ajuda do Kaspersky Endpoint Security.
  - **Botão**. Ao clicar neste botão é aberta a janela **Suporte**, que contém as informações sobre o sistema operacional, a versão do Kaspersky Endpoint Security, e que direciona você aos recursos de informações da Kaspersky.
  - **Botão** / . Ao clicar neste botão é aberta a janela **Licenciamento**, com informações sobre a licença atual.
  - **Botão** / / Um clique nesse botão abre a janela **Eventos** que contém informações sobre as atualizações disponíveis, bem como solicitações para acessar dispositivos e arquivos criptografados.

O botão só fica disponível quando há solicitações de acesso ou atualizações desinstaladas.



Janela principal do aplicativo

Para abrir a janela principal do Kaspersky Endpoint Security, execute uma das seguintes ações:

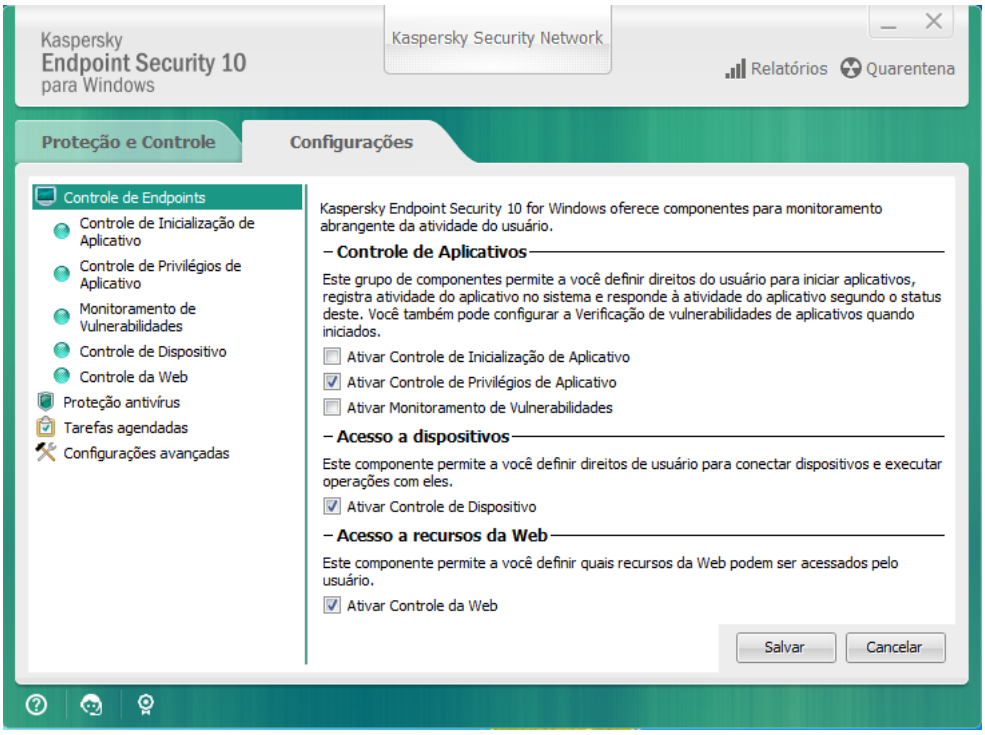
- Clique no ícone de aplicativo na área de notificação da barra de tarefas do Microsoft Windows.
- Selecione **Kaspersky Endpoint Security 10 for Windows** no menu de contexto do ícone de aplicativo.

Guia Configurar configuração do aplicativo

A guia de configurações do Kaspersky Endpoint Security permite definir as configurações gerais do aplicativo, os componentes individuais, os relatórios e armazenamentos, as tarefas de verificação, as tarefas de atualização, as tarefas de verificação de vulnerabilidades e a comunicação com os servidores do Kaspersky Security Network.

A guia de configurações do aplicativo é constituída por duas partes (veja a figura seguinte):

- A parte esquerda contém os componentes do aplicativo, as tarefas e uma seção de configurações avançadas composta de várias subseções.
- A parte direita contém elementos de controle que você pode usar para definir as configurações do componente ou tarefa selecionada na parte esquerda da janela, bem como configurações avançadas.



Guia Configurar configuração do aplicativo

Para abrir a guia das configurações do aplicativo, execute uma das seguintes ações:

- Na janela principal do aplicativo, selecione a guia **Configurações**.
- No menu de contexto do ícone de aplicativo, selecione **Configurações**.

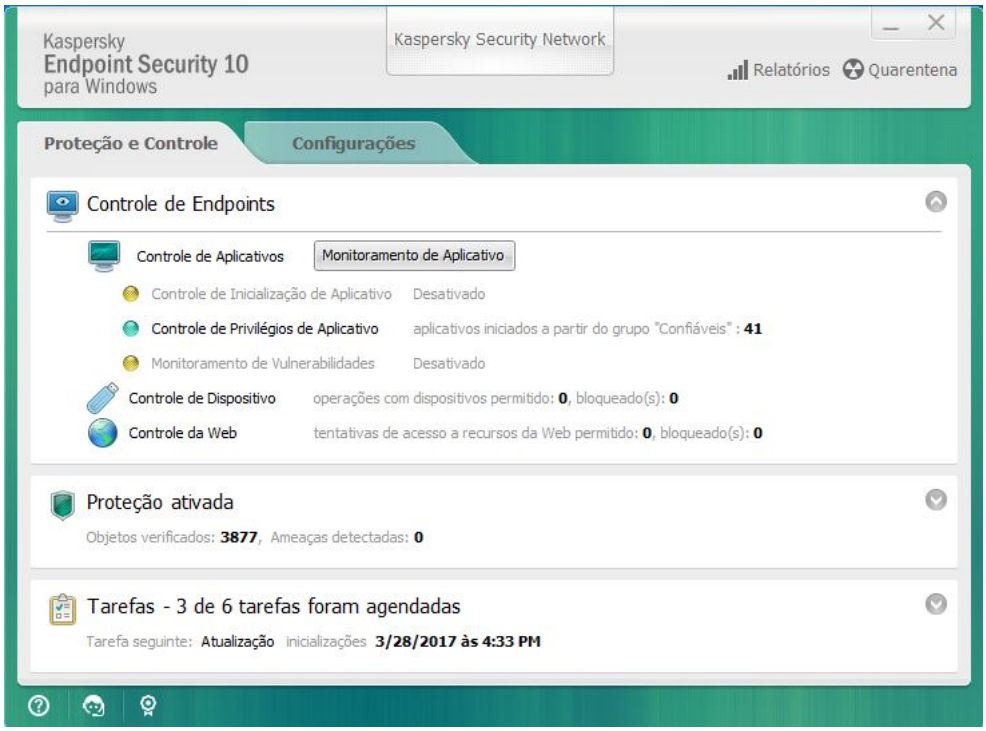
Guia Proteção e Controle de aplicativo

A guia Proteção e Controle do Kaspersky Endpoint Security é destinada a fornecer a informação geral sobre o desempenho de todas as tarefas e a operação de todos os componentes de aplicativo. Nessa guia, você também pode regular a operação de componentes e o desempenho de tarefas.

A guia Proteção e Controle de aplicativo é composta por três partes (veja a figura abaixo):

- A seção **Controle de Endpoints** contém uma lista de componentes de controle.
- A seção **Gerenciar proteção** contém uma lista de componentes da Proteção Antivírus.
- A seção **Tarefas** contém uma lista de tarefas locais que são executadas no computador.

Cada seção contém elementos de controle que você pode usar para ativar ou desativar a operação de um componente, vá às configurações do componente selecionado ou tarefa e exiba estatísticas operacionais do componente ou da tarefa selecionada.



Guia Proteção e Controle de aplicativo

Para abrir a guia Proteção e Controle de aplicativo, execute uma das seguintes ações:

- Na janela do aplicativo principal, selecione a guia **Proteção e Controle**.
- Clique no ícone de aplicativo na área de notificação da barra de tarefas do Microsoft Windows.
- Selecione **Kaspersky Endpoint Security 10 for Windows** no menu de contexto do ícone de aplicativo.

Licenciamento do aplicativo

Esta seção fornece informações sobre os conceitos gerais relacionados à licença do aplicativo.

Sobre o Contrato de Licença do Usuário Final

O *Contrato de Licença do Usuário Final* é um acordo vinculativo entre você e a AO Kaspersky Lab que estipula os termos de uso do aplicativo.

É recomendável ler os termos do contrato de licença com atenção antes de começar a usar o aplicativo.

Você pode ver os termos do Contrato de Licença das seguintes formas:

- Quando instalar o Kaspersky Endpoint Security no modo interativo.
- Lendo o arquivo license.txt. Este documento está incluído no kit de distribuição de aplicativo.

Confirmar que concorda com o Contrato de Licença do Usuário Final ao instalar o aplicativo significa que você aceita os termos do Contrato de Licença do Usuário Final. Se você não aceitar os termos do Contrato de Licença do Usuário Final, será preciso cancelar a instalação.

Sobre a licença

A *licença* refere-se ao direito de usar o aplicativo por um período determinado, que é concedido nos termos do Contrato de Licença do Usuário Final.

A licença válida confere o direito aos seguintes tipos de serviços:

- Uso do aplicativo de acordo com os termos do Contrato de Licença do Usuário Final
- Suporte Técnico

O âmbito dos serviços e os termos de condições de uso do aplicativo dependem do tipo da licença sob a qual o aplicativo foi ativado.

Os seguintes tipos de licença são disponibilizados:

- *Avaliação* – uma licença gratuita destinada para a avaliação do aplicativo.

  Uma licença de avaliação geralmente tem um termo curto. Quando a licença de avaliação expira, todos os recursos do aplicativo do Kaspersky Endpoint Security são desativados. Para continuar a usar o aplicativo, é necessário comprar uma licença comercial.

  O aplicativo só pode ser ativado uma vez usando uma licença de avaliação.

- *Comercial* – uma licença paga que é fornecida quando você compra o Kaspersky Endpoint Security.

  A funcionalidade do aplicativo que está disponível com uma licença comercial depende da escolha do produto. O produto selecionado é indicado no Certificado de Licença. As informações sobre os produtos disponíveis podem ser encontradas no site da Kaspersky.

Quando a licença comercial expira, os recursos principais do aplicativo são desativados. Para continuar a usar o aplicativo, é necessário renovar a licença comercial. Se você não planeja renovar a licença, é necessário remover o aplicativo do computador.

Sobre o certificado de licença

Um *certificado de licença* é um documento transferido para o usuário em conjunto com um arquivo de chave ou um código de ativação.

O certificado de licença contém as seguintes informações de licença:

- Número de ordem
- Detalhes do usuário a quem a licença é concedida
- Detalhes do aplicativo que pode ser ativado usando a licença
- A limitação no número de unidades licenciadas (por exemplo, o número de dispositivos nos quais o aplicativo pode ser usado mediante a licença)
- Data de início do termo da licença
- Data de expiração da licença ou do termo da licença
- Tipo de licença

Sobre a assinatura

A *Assinatura do Kaspersky Endpoint Security* é uma compra do aplicativo com parâmetros específicos (data de expiração da assinatura, número de dispositivos protegidos). Você pode solicitar a assinatura do Kaspersky Endpoint Security junto a seu provedor de serviço (como seu ISP, por exemplo). A assinatura pode ser renovada manualmente ou automaticamente ou você poderá cancelá-la. Você pode gerenciar a sua assinatura no site do provedor de serviços.

A assinatura pode ser limitada (por um ano, por exemplo) ou ilimitada (sem uma data de expiração). Para manter o Kaspersky Endpoint Security a funcionar após a expiração do termo da assinatura limitada, você deve renovar sua assinatura. A assinatura ilimitada é automaticamente renovada se os serviços do fornecedor forem pagos antecipadamente.

No caso de assinatura limitada, após sua expiração, você poderá ter um período de carência para renovar a assinatura, durante o qual o aplicativo mantém sua funcionalidade completa. O provedor do serviço decide se deve conceder um período de carência ou não e, caso ele seja concedido, determina a duração do período de carência.

Para usar o Kaspersky Endpoint Security com assinatura, você deve aplicar o código de ativação recebido do provedor do serviço. Após o código de ativação ser aplicado, a chave ativa é instalada. A chave ativa define a licença para usar o aplicativo com uma assinatura. Uma chave adicional pode ser instalada somente usando um código de ativação e não pode ser instalada usando um arquivo de chave ou com uma assinatura.

A funcionalidade do aplicativo disponível com a assinatura pode corresponder à funcionalidade do aplicativo para os seguintes tipos de licenças comerciais: Padrão, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Licenças destes tipos foram concebidas para proteger servidores de arquivos, estações de trabalho e dispositivos móveis, e suportam o uso de componentes de controle em estações de trabalho e dispositivos móveis.

As possíveis opções de gerenciamento da assinatura podem variar consoante o provedor do serviço. O provedor do serviço poderá não oferecer um período de carência para renovar a assinatura, durante o qual o aplicativo mantém sua funcionalidade.

Os códigos de ativação comprados com a assinatura podem não ser usados para ativar versões anteriores do Kaspersky Endpoint Security.

Sobre o código de ativação

Um *código de ativação* é uma sequência alfanumérica exclusiva de vinte letras e numerais latinos que você recebe ao comprar uma licença comercial do Kaspersky Endpoint Security.

Para ativar o aplicativo utilizando o código de ativação, é necessário acesso à Internet para se conectar aos servidores de ativação da Kaspersky.

Quando o aplicativo é ativado usando um código de ativação, a chave ativa é instalada. Uma chave adicional pode ser instalada somente usando um código de ativação e não pode ser instalada usando um arquivo de chave ou com uma assinatura.

Se o código de ativação tiver sido perdido após a ativação do aplicativo, você pode restaurar o código de ativação. Pode ser necessário um código de ativação, por exemplo, para registrar um Kaspersky CompanyAccount. Para restaurar um código de ativação, você deve contatar o Suporte técnico da Kaspersky.

Sobre a chave

Uma *chave* é uma sequência alfanumérica exclusiva. A chave torna possível usar o aplicativo nos termos do Certificado de Licença (tipo de licença, termo de validade da licença, restrições da licença).

Um certificado de licença não é fornecido para uma chave instalada com assinatura.

Uma chave pode ser adicionada ao aplicativo usando um código de ativação ou um arquivo de chave.

Você pode adicionar, editar ou excluir chaves. A chave pode ser bloqueada pela Kaspersky se os termos do Contrato de Licença do Usuário Final forem violados. Se a chave for adicionada à lista negra, você terá de adicionar uma chave diferente para continuar a usar o aplicativo.

Se uma chave para uma licença expirada tiver sido excluída, a funcionalidade do aplicativo ficará indisponível. Você não pode adicionar tal chave novamente depois que ela foi apagada.

Há dois tipos de chaves: ativa e adicional.

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

Uma *chave adicional* é uma chave que dá ao usuário direito para usar o aplicativo, mas que não está atualmente em uso. Após a chave ativa expirar, uma chave adicional fica automaticamente ativa. Uma chave adicional somente pode ser adicionada se a chave ativa estiver disponível.

Uma chave da licença de avaliação pode ser adicionada somente como uma chave ativa. Não é possível adicioná-la como chave adicional. Uma licença de avaliação não pode substituir a chave ativa para uma licença comercial.

Se uma chave for colocada na lista negra, a funcionalidade do aplicativo definida pela licença com que o aplicativo foi ativado permanece disponível durante oito dias. O Kaspersky Security Network e as atualizações do banco de dados e do módulo do aplicativo estão disponíveis sem restrições. O aplicativo notifica o usuário de que a chave foi adicionada à lista negra. Após oito dias, a funcionalidade do aplicativo se torna limitada no nível de funcionalidade que estiver disponível após a expiração do termo da licença: o aplicativo é executado sem atualizações e o Kaspersky Security Network não estará disponível.

Sobre o arquivo de chave

Um *arquivo de chave* é um arquivo com a extensão .key que você recebe da Kaspersky após comprar o Kaspersky Endpoint Security. A finalidade de um arquivo de chave é adicionar uma chave que ativa o aplicativo.

Não é necessário conectar-se aos servidores de ativação da Kaspersky para ativar o aplicativo com um arquivo de chave.

Você pode recuperar um arquivo de chave caso ele seja excluído acidentalmente. Talvez você precise de um arquivo de chave para registrar um Kaspersky CompanyAccount, por exemplo.

Para recuperar um arquivo de chave, realize uma das seguintes ações:

- Entre em contato com o vendedor da licença.
- Adquira um arquivo de chave no site da Kaspersky com base no código de ativação existente.

Quando o aplicativo é ativado usando um arquivo de chave, uma chave ativa é adicionada. Uma chave de licença reserva só pode ser adicionada usando um arquivo de chave e não pode ser adicionada usando um código de ativação.

Sobre o fornecimento de dados

Ao aceitar o Contrato de Licença do Usuário Final, você aceita transferir automaticamente informações sobre o seu uso do produto, bem como o tipo, versão e localização linguística do programa instalado, o identificador exclusivo do instalador de programas e o tipo da instalação, além de dados sobre chaves ativas e adicionais (inclusive o tipo de licença, período de validade, a data da ativação do programa e data de expiração da licença, o número da licença, o estado atual da licença, a versão do protocolo de interação do servidor de ativação).

Se o programa for ativado com um código de ativação, para receber informações estatísticas sobre a distribuição e o uso dos produtos do Titular da Licença, você aceita fornecer automaticamente a versão do programa que está sendo utilizada (inclusive informações sobre atualizações de programas instaladas, o identificador de Instalação do programa e informações sobre licenças), a versão do sistema operacional e identificadores de componentes do programa ativos no momento em que as informações são fornecidas.

As informações recebidas são protegidas pela Kaspersky conforme a lei e os requisitos e as regulações aplicáveis da Kaspersky.

A Kaspersky usa somente informações recebidas anonimamente e apenas na forma de dados estatísticos gerais. As estatísticas gerais são geradas automaticamente utilizando informações originais coletadas e não contêm nenhum dado pessoal ou outras informações confidenciais. As informações originalmente reunidas são destruídas na forma como são acumuladas (uma vez por ano). Os dados estatísticos gerais são guardados indefinidamente.

Leia o Contrato de Licença do Usuário Final e visite o site da Kaspersky http://brazil.kaspersky.com/privacy para saber mais sobre como nós coletamos, processamos, armazenamos e destruímos informações sobre o uso do aplicativo após você aceitar o Contrato de Licença do Usuário Final e concordar com a Declaração KSN. Os arquivos license.txt e ksn.txt contêm o Contrato de Licença do Usuário Final e a Declaração KSN e fazem parte do pacote de distribuição de programas.

Exibir informações da licença

Para exibir as informações da licença:

1. Abra a janela principal do aplicativo.
2. Clique no botão / na parte inferior da janela principal do aplicativo.

   A janela **Licenciamento** abre. As informações da licença são exibidas na seção na parte superior da janela **Licenciamento**.

Comprar uma licença

É possível comprar uma licença após a instalação do aplicativo. Ao comprar uma licença, você recebe um código de ativação ou um arquivo de chave para ativar o aplicativo.

Para comprar uma licença:

1. Abra a janela principal do aplicativo.
2. Clique no botão / na parte inferior da janela principal do aplicativo.

   A janela **Licenciamento** abre.
3. Na janela **Licenciamento**, execute uma das seguintes operações:

   - Se nenhuma chave foi adicionada ou se uma chave para uma licença de avaliação foi adicionada, clique no botão **Comprar licença**.
   - Se a chave da licença comercial foi adicionada, clique no botão **Renovar licença**.

   Será aberta uma janela com o site da loja on-line da Kaspersky, onde você poderá comprar a licença.

Renovar uma licença

Ao se aproximar a data de expiração da licença, é possível renová-la. A renovação permite manter o computador protegido depois da expiração da licença atual e até você ativar o aplicativo sob uma nova licença.

Para renovar uma licença:

1. Recebe um novo código de ativação do aplicativo ou arquivo de chave.
2. Adicione uma chave adicional com o código de ativação ou o arquivo de chave que você recebeu.

   Como resultado, uma chave adicional é adicionada. Ela se torna ativa após a expiração da licença.

Poderá demorar algum tempo para que a chave seja atualizada de adicional para ativa, devido à distribuição da carga pelos servidores de ativação da Kaspersky.

Renovar a assinatura

Quando você usa o aplicativo com uma assinatura, o Kaspersky Endpoint Security contata automaticamente o servidor de ativação em intervalos específicos até que sua assinatura expire.

Se você usar o aplicativo com uma assinatura ilimitada, o Kaspersky Endpoint Security verifica automaticamente o servidor de ativação para detectar chaves renovadas no modo de segundo plano. Se uma chave estiver disponível no servidor de ativação, o aplicativo adiciona-a substituindo a chave anterior. Dessa forma, a assinatura ilimitada do Kaspersky Endpoint Security é renovada sem envolvimento do usuário.

Se você usar o aplicativo com uma assinatura ilimitada, no dia em que a assinatura (ou o período de carência após a expiração durante o qual a renovação da assinatura está disponível) expira, o Kaspersky Endpoint Security exibe uma notificação correspondente e deixa de tentar renovar a assinatura automaticamente. Nesse caso, o Kaspersky Endpoint Security comporta-se da mesma forma como quando uma licença comercial do aplicativo expira: o aplicativo é executado sem atualizações e o Kaspersky Security Network fica indisponível.

Você pode renovar a assinatura no site do provedor de serviços.

Você pode atualizar o status da subscrição manualmente na janela **Licenciamento**. Isso poderá ser necessário se a assinatura tiver sido renovada após a expiração do período de carência e o aplicativo não tiver atualizado o status da assinatura automaticamente.

Visitar o site do provedor de serviço

Para visitar o site do provedor do serviço a partir da interface do aplicativo:

1. Abra a janela principal do aplicativo.
2. Clique no botão / na parte inferior da janela principal do aplicativo.

   A janela **Licenciamento** abre.

3. Na janela **Licenciamento**, clique em **Entrar em contato com o provedor de assinaturas**.

Sobre os métodos de ativação do aplicativo

Ativação é um processo que aplica uma licença, a qual permite que você use uma versão totalmente funcional do aplicativo, até que a licença expire. O processo de ativação do aplicativo envolve a adição de uma chave.

O aplicativo é ativado das seguintes formas:

- Quando instalar o aplicativo, com a ajuda do Assistente de Configuração Inicial. Você pode adicionar a chave ativa desta forma.
- Localmente da interface de aplicativo, usando o Assistente de Ativação Você pode adicionar tanto a chave ativa como a chave adicional deste modo.
- Remotamente com o conjunto de software do Kaspersky Security Center criando e depois iniciando uma tarefa adicionar chave. Você pode adicionar a chave ativa e a chave adicional dessa forma.
- Remotamente, distribuindo chaves e códigos de ativação que estão armazenados no armazenamento de chaves no Servidor de Administração do Kaspersky Security Center para computadores clientes (consultar o *Manual do Administrador do Kaspersky Security Center* para obter mais informações). Você pode adicionar a chave ativa e a chave adicional dessa forma.

  O código de ativação comprado com assinatura é distribuído em primeiro lugar.

- Usando a linha de comando.

Poderá demorar algum tempo até que o aplicativo seja ativado com um código de ativação (durante a instalação remota ou não interativa) devido à distribuição de carga pelos servidores de ativação da Kaspersky. Se você precisar ativar o aplicativo de imediato, você poderá interromper o processo de ativação em andamento e iniciar a ativação usando o Assistente de Ativação.

Usar o Assistente de Ativação para ativar o aplicativo

Para ativar o Kaspersky Endpoint Security usando o Assistente de Ativação:

1. Clique no botão / na parte inferior da janela principal do aplicativo.

   A janela **Licenciamento** abre.

2. Na janela **Licenciamento**, clique no botão **Ativar o aplicativo sob uma nova licença**.

   O Assistente de Ativação do aplicativo é iniciado.

3. Siga as instruções do Assistente de Ativação.

Para obter informações mais detalhadas sobre o procedimento de ativação do aplicativo, consulte a seção no Assistente de Configuração Inicial.

Ativar o aplicativo a partir da linha de comando

Para ativar o aplicativo a partir da linha de comando,

digite `avp.com license /add <código de ativação ou arquivo de chave> /password=<senha>` na linha de comando.

Iniciar e interromper o aplicativo

Esta seção descreve como configurar a inicialização automática do aplicativo, iniciar ou encerrar o aplicativo manualmente e pausar ou continuar a proteção e controle de componentes.

Ativar e desativar a inicialização automática do aplicativo

A inicialização automática significa que o Kaspersky Endpoint Security é iniciado logo após a inicialização do sistema operacional, sem haver ação do usuário. Esta opção de inicialização automática está ativa por padrão.

Após a instalação, o Kaspersky Endpoint Security é iniciado pela primeira vez automaticamente. Daqui em diante, o aplicativo iniciará automaticamente após a inicialização do sistema operacional.

O download de bancos de dados do Antivírus de Kaspersky Endpoint Security após o início do sistema operacional pode levar até dois minutos, dependendo dos recursos do computador. Durante este tempo, o nível da proteção do computador é reduzido. O download de bancos de dados do antivírus quando Kaspersky Endpoint Security é iniciado em um sistema operacional já carregado não causa uma redução do nível de proteção do computador.

Para ativar ou desativar a inicialização automática do sistema operacional:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Proteção antivírus** à esquerda.

   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Execute uma das seguintes ações:

   - Se desejar ativar a inicialização automática do aplicativo, marque a caixa de seleção **Iniciar o Kaspersky Endpoint Security 10 for Windows na inicialização do computador**.
   - Se desejar desativar a execução automática do aplicativo, desmarque a caixa de seleção **Iniciar o Kaspersky Endpoint Security 10 for Windows na inicialização do computador**.
4. Para salvar as alterações, clique no botão **Salvar**.

Iniciar e interromper o aplicativo manualmente

Os especialistas da Kaspersky não recomendam encerrar o Kaspersky Endpoint Security manualmente, pois ao fazê-lo você estará expondo o computador e seus dados pessoais a ameaças. Se necessário, você pode pausar a proteção do computador por quanto tempo precisar, sem parar o aplicativo.

O Kaspersky Endpoint Security deve ser iniciado manualmente se você tiver desativado anteriormente a inicialização automática do aplicativo.

Para iniciar o aplicativo manualmente,

No menu **Iniciar**, selecione **Aplicativos** → **Kaspersky Endpoint Security 10 for Windows**.

Para encerrar o aplicativo manualmente:

1. Clique com o botão direito do mouse para abrir o ícone do menu de contexto do aplicativo que está na área de notificação da barra de tarefas.
2. No menu de contexto, selecione **Sair**.

Pausar e reiniciar a Proteção e Controle do computador

Pausar a Proteção e o Controle do computador significa desativar todos os componentes de Proteção e Controle do Kaspersky Endpoint Security durante certo tempo.

O status de aplicativo é exibido usando o ícone de aplicativo na área de notificação da barra de tarefas.

- O ícone indica que a proteção e o controle do computador foram pausados.
- O ícone indica que a proteção e o controle do computador estão desativados.

Pausar ou continuar a Proteção e Controle do computador não afeta as tarefas de verificação e atualização.

Se nenhuma conexão de rede for estabelecida no momento da pausa ou continuação da Proteção e Controle do computador, é exibida uma notificação sobre o término destas conexões de rede.

Para pausar a Proteção e Controle do computador:

1. Clique com o botão direito do mouse para abrir o ícone do menu de contexto do aplicativo que está na área de notificação da barra de tarefas.
2. No menu de contexto, selecione **Pausar a Proteção e Controle**.

   A janela **Pausar a proteção** é aberta.
3. Selecione uma das seguintes opções:

   - **Pausar pelo tempo especificado** – A Proteção e o Controle do computador são reiniciados após decorrer o tempo especificado na lista suspensa abaixo.
   - **Pausar até reiniciar** – A Proteção e Controle do computador é continuada após você fechar e reabrir o aplicativo ou reiniciar o sistema operacional. A inicialização automática do aplicativo precisa ser ativada para que esta opção possa ser usada.
   - **Pausar** – A Proteção e Controle do computador é continuada quando você decide reativá-la.
4. Se você tiver selecionado a opção **Pausar pelo tempo especificado** na etapa anterior, selecione o intervalo necessário na lista suspensa.

Para reiniciar a proteção e controle do computador:

1. Clique com o botão direito do mouse para abrir o ícone do menu de contexto do aplicativo que está na área de notificação da barra de tarefas.
2. No menu de contexto, selecione **Continuar a Proteção e Controle**.

Você pode decidir continuar a Proteção e Controle do computador a qualquer momento, seja qual for a opção de pausa de proteção e controle que tenha selecionado anteriormente.

Proteger o sistema de arquivos do computador. Antivírus de Arquivos

Esta seção contém informações sobre o Antivírus de Arquivos e as instruções para definir as configurações do componente.

Sobre o Antivírus de Arquivos

O Antivírus de Arquivos evita a infecção do sistema de arquivos do computador. Por padrão, o Antivírus de Arquivos inicia juntamente com o Kaspersky Endpoint Security, permanece sempre na memória do computador e verifica todos os arquivos que são abertos, salvos ou executados no computador e em todas as unidades conectadas, para detectar a presença de vírus e outras ameaças.

Ao detectar uma ameaça em um arquivo, o Kaspersky Endpoint Security executa as seguintes operações:

1. Identifica o tipo de objeto detectado no arquivo (como um *vírus* ou *Cavalo de troia*).
2. Rotula o arquivo como *provavelmente infectado* caso a verificação não consiga determinar se o arquivo está ou não infectado. O arquivo pode conter uma sequência de código que é típica de vírus ou outro tipo de malware, ou o código modificado de um vírus conhecido.
3. O aplicativo exibe uma notificação sobre o objeto malicioso detectado no arquivo (se as notificações forem configuradas), e processa o arquivo adotando a ação especificada em configurações de Antivírus de Arquivos.

Ativar e desativar o Antivírus de Arquivos

Por padrão, o Antivírus de Arquivos está ativo e é executado no modo recomendado pelos especialistas da Kaspersky. Se necessário, você pode desativar o Antivírus de Arquivos.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

Para ativar ou desativar o Antivírus de Arquivos na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Proteção**.

   A seção **Proteção** é exibida.
4. Clique com o botão direito do mouse para abrir o menu de contexto da linha com as informações sobre o componente Antivírus de Arquivos.

   Será aberto um menu para a seleção de ações.
5. Execute uma das seguintes ações:

   - Para ativar o Antivírus de Arquivos, selecione **Iniciar** no menu.

O ícone de status do componente , exibido à esquerda na linha do **Antivírus de Arquivos**, muda para o ícone .

- Para desativar o Antivírus de Arquivos, selecione **Interromper** no menu.

  O ícone de status do componente , exibido à esquerda na linha do **Antivírus de Arquivos**, muda para o ícone .

Para ativar ou desativar o Antivírus de Arquivos na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de Arquivos**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de Arquivos.
3. Execute uma das seguintes ações:
   - Se desejar ativar o Antivírus de Arquivos, marque a caixa de seleção **Ativar Antivírus de Arquivos**.
   - Se desejar desativar o Antivírus de Arquivos, desmarque a caixa de seleção **Ativar Antivírus de Arquivos**.
4. Para salvar as alterações, clique no botão **Salvar**.

Pausar automaticamente Antivírus de Arquivos

Você pode configurar o Antivírus de Arquivos para pausar automaticamente em um horário especificado ou quando estiver lidando com determinados programas.

Pausar o Antivírus de Arquivos quando ele estiver em conflito com outros programas é uma operação emergencial. Na existência de conflitos durante a operação de um componente, é recomendável entrar em contato com o Suporte Técnico da Kaspersky (https://companyaccount.kaspersky.com). Os especialistas do Suporte Técnico o ajudarão a configurar o Antivírus de Arquivos para que este seja executado simultaneamente com outros programas no computador.

Para configurar a pausa automática do Antivírus de Arquivos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de Arquivos**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de Arquivos.
3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   A janela **Antivírus de Arquivos** abre.
4. Na janela **Antivírus de Arquivos**, selecione a guia **Adicional**.
5. Na seção **Pausar tarefa**:
   - Para configurar a pausa automática do Antivírus de Arquivos em uma hora especificada, marque a caixa de seleção **Por agendamento** e clique no botão **Agendamento**.

     A janela **Pausar tarefa** abre.

- Para configurar a pausa automática do Antivírus de Arquivos na inicialização de determinados aplicativos, marque a caixa de seleção **Ao iniciar o aplicativo** e clique no botão **Selecionar**.

  A janela **Aplicativos** abre.

6. Execute uma das seguintes ações:

   - Para configurar a pausa automática do Antivírus de Arquivos em uma hora especificada, na janela **Pausar tarefa**, utilize os campos **Pausar tarefa às** e **Reiniciar tarefa às** para especificar o período de tempo (no formato HH:MM) durante o qual o Antivírus de Arquivos ficará pausado. Clique em **OK**.

   - Para configurar a pausa automática do Antivírus de Arquivos na inicialização de determinados aplicativos, use os botões **Adicionar**, **Editar** e **Remover** na janela **Aplicativos** para criar uma lista de aplicativos que terão a execução do Antivírus de Arquivos pausada. Clique em **OK**.

7. Na janela **Antivírus de Arquivos**, clique em **OK**.

8. Para salvar as alterações, clique no botão **Salvar**.

Configurar Antivírus de Arquivos

Você pode executar as seguintes ações para configurar o Antivírus de Arquivos:

- Alterar o nível de segurança.

  Você pode selecionar um dos níveis de segurança pré-configurados ou definir manualmente configurações de nível de segurança. A alteração das configurações do nível de segurança não impede a reversão para as configurações de nível recomendado.

- Alterar a ação executada pelo Antivírus de Arquivos quando um arquivo infectado for detectado.

- Editar o escopo de proteção do Antivírus de Arquivos.

  Expanda ou restrinja o escopo de proteção ao adicionar ou remover objetos de verificação, ou ao alterar o tipo de arquivos para verificação.

- Configurar o Analisador Heurístico.

  O Antivírus de Arquivos utiliza um método chamado análise de assinaturas. Na análise de assinaturas, o Antivírus de Arquivos compara o objeto detectado com os registros do banco de dados. De acordo com as recomendações dos especialistas da Kaspersky, a análise de assinaturas está sempre ativada.

  Para aumentar a eficácia da proteção, você pode usar a análise heurística. Durante a análise heurística, o Antivírus de Arquivos analisa a atividade de objetos no sistema operacional. A análise heurística permite detectar objetos maliciosos para os quais nenhum registro está disponível atualmente nos bancos de dados de antivírus do aplicativo.

- Otimizar a verificação.

  Com a otimização da verificação de arquivos, que é executada pelo Antivírus de Arquivos, é possível reduzir o tempo da verificação e aumentar a velocidade de processamento do Kaspersky Endpoint Security. Isso é possível quando são verificados apenas os arquivos novos e aqueles que foram alterados após a verificação anterior. Esse modo se aplica a arquivos simples e compostos.

  Você também pode ativar as tecnologias iChecker e iSwift, que aumentam a velocidade das verificações por meio da exclusão de arquivos que permaneceram inalterados após a última verificação.

- Configurar a verificação dos arquivos compostos.

- Alterar o modo de verificação dos arquivos.

Como alterar o nível de segurança

Para proteger o sistema de arquivos do computador, o Antivírus de Arquivos emprega vários grupos de configurações. Estes grupo de configurações são chamados *níveis de segurança*. Há três níveis de segurança pré-configurados: **Alto**, **Recomendado** e **Baixo**. As configurações do nível de segurança **Recomendado** são consideradas as melhores configurações recomendadas pelos especialistas da Kaspersky.

Para modificar um nível de segurança:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de Arquivos**.
   Na parte direita da janela, são exibidas as configurações do componente Antivírus de Arquivos.
3. Na seção **Nível de segurança**, execute uma das seguintes operações:
   - Se você quiser estabelecer um dos níveis de segurança pré-configurados (**Alto**, **Recomendado** ou **Baixo**), selecione-o com o controle deslizante.
   - Se quiser configurar um nível de segurança personalizado, clique no botão **Configurações** e, na janela **Antivírus de Arquivos** exibida, insira as configurações personalizadas.
     Após configurar um nível de segurança personalizado, o nome do nível de segurança, na seção de **Nível de segurança**, muda para **Personalizado**.
   - Se quiser alterar o nível de segurança de e-mails para **Recomendado**, clique no botão **Padrão**.
4. Para salvar as alterações, clique no botão **Salvar**.

Alterar a ação do Antivírus de Arquivos executada em arquivos infectados

Para alterar a ação do Antivírus de Arquivos executada em arquivos infectados:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de Arquivos**.
   Na parte direita da janela, são exibidas as configurações do componente Antivírus de Arquivos.
3. Na seção **Ação ao detectar ameaça**, selecione a opção desejada:
   - **Selecionar ação automaticamente**.
   - **Executar ação: Desinfectar. Excluir se a desinfecção falhar**.
   - **Executar ação: Desinfectar.**

Ainda que esta opção não esteja selecionada, o Kaspersky Endpoint Security aplica a ação **Remover** aos arquivos que são parte do aplicativo Windows Store.

- **Executar ação: Remover**.
- **Executar ação: Bloquear**.

4. Para salvar as alterações, clique no botão **Salvar**.

Editar o escopo de proteção do Antivírus de Arquivos.

O escopo de proteção refere-se aos objetos que o componente verifica quando está ativado. O escopo de proteção de componentes diferentes tem propriedades diversas. O local e o tipo de arquivos a serem verificados são propriedades do escopo de proteção do Antivírus de Arquivos. Por padrão, o Antivírus de Arquivos verifica somente arquivos que podem ser infectados que estão armazenados em discos rígidos, unidades de rede ou mídia removível.

Para criar o escopo de proteção:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de Arquivos**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de Arquivos.
3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   A janela **Antivírus de Arquivos** abre.
4. Na janela **Antivírus de Arquivos**, selecione a guia **Geral**.
5. Na seção **Tipos de arquivos**, especifique o tipo de arquivo que você deseja que o Antivírus de Arquivos verifique:

   - Para verificar todos os arquivos, selecione **Todos os arquivos**.
   - Para verificar os arquivos nos formatos com risco maior de infecção, selecione **Arquivos verificados por formato**.
   - Para verificar os arquivos com as extensões com risco maior de infecção, selecione **Arquivos verificados por extensão**.

   Ao selecionar o tipo de arquivos a verificar, lembre-se das seguintes informações:

   - Existem alguns formatos de arquivos (como .txt) em que a probabilidade de intrusão de código malicioso e a ativação subsequente é bastante baixa. Ao mesmo tempo, há formatos de arquivos que contêm ou que talvez contenham um código executável (como .exe, .dll e doc). O risco de infiltração e ativação de código malicioso nesses arquivos é bastante grande.
   - O invasor talvez envie vírus ou outro tipo de programa malicioso para o computador em um arquivo executável renomeado com a extensão .txt. Ao selecionar a verificação de arquivos por extensão, este arquivo é ignorado da verificação. Ao selecionar a verificação de arquivos por formato, o Antivírus de

Arquivos, seja qual for a extensão, analisa o cabeçalho do arquivo. A análise descobre se o arquivo está em formato .exe. Este arquivo é verificado cuidadosamente para detectar vírus e outro tipo de malware.

6. Na lista **Escopo de proteção**, execute uma das seguintes operações:

   - Se desejar adicionar um novo objeto ao escopo da verificação, clique no botão **Adicionar**.
   - Se desejar alterar o local do objeto, selecione o objeto no escopo da verificação e clique no botão **Editar**.

   A janela **Selecionar escopo da verificação** é exibida.

   - Se desejar remover um objeto da lista de objetos a serem verificados, selecione um na lista de objetos a serem verificados e clique no botão **Remover**.

     É exibida uma janela para confirmar exclusão.

7. Execute uma das seguintes ações:

   - Se desejar adicionar um novo objeto ou alterar o local de um objeto na lista de objetos a serem verificados, selecione o objeto na janela **Selecionar escopo da verificação** e clique no botão **Adicionar**.

     Todos os objetos selecionados na janela **Selecionar escopo da verificação** serão exibidos na janela **Antivírus de Arquivos** na lista **Escopo de proteção**.

     Clique em **OK**.

   - Se desejar remover um objeto, clique no botão **Sim** na janela de confirmação de remoção.

8. Repita as etapas 6 a 7, se necessário, para adicionar, mover ou remover objetos da lista de objetos a serem verificados.

9. Para excluir um objeto da lista de objetos a serem verificados, desmarque a caixa de seleção próxima ao objeto na lista **Escopo de proteção**. Contudo, o objeto permanecerá na lista de objetos a serem verificados, mesmo sendo excluído da verificação pelo Antivírus de Arquivos.

10. Na janela **Antivírus de Arquivos**, clique em **OK**.

11. Para salvar as alterações, clique no botão **Salvar**.

Usar o Analisador Heurístico com Antivírus de Arquivos

Para configurar a utilização do Analisador Heurístico na operação do Antivírus de Arquivos:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de Arquivos**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de Arquivos.

3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   A janela **Antivírus de Arquivos** abre.

4. Na janela **Antivírus de Arquivos**, selecione a guia **Desempenho**.

5. Na seção **Métodos de verificação**:

- Se desejar usar a análise heurística no Antivírus de Arquivos, marque a caixa de seleção **Análise Heurística** e use a barra deslizante para definir o nível de detalhamento da análise heurística: **Verificação superficial**, **Verificação média** ou **Verificação profunda**.
- Se não desejar usar a análise heurística no Antivírus de Arquivos, desmarque a caixa de seleção **Análise Heurística**.

6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Usar tecnologias de verificação na operação do Antivírus de Arquivos

Para configurar a utilização de tecnologias de verificação na operação do Antivírus de Arquivos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de Arquivos**.
   Na parte direita da janela, são exibidas as configurações do componente Antivírus de Arquivos.
3. Na seção **Nível de segurança**, clique no botão **Configurações**.
   A janela **Antivírus de Arquivos** abre.
4. Na janela **Antivírus de Arquivos**, selecione a guia **Adicional**.
5. Na seção **Tecnologias de verificação**:
   - Marque as caixas de seleção ao lado dos nomes das tecnologias que deseja usar na operação do Antivírus de Arquivos.
   - Desmarque as caixas de seleção ao lado dos nomes das tecnologias que não deseja usar na operação do Antivírus de Arquivos.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Otimizar a verificação do arquivo

Para otimizar a verificação de arquivos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de Arquivos**.
   Na parte direita da janela, são exibidas as configurações do componente Antivírus de Arquivos.
3. Clique no botão **Configurações**.
   A janela **Antivírus de Arquivos** abre.

4. Na janela **Antivírus de Arquivos**, selecione a guia **Desempenho**.

5. Na seção **Otimização da verificação**, marque a caixa de seleção **Verificar somente arquivos novos e alterados**.

6. Clique em **OK**.

7. Para salvar as alterações, clique no botão **Salvar**.

Verificar arquivos compostos

Uma técnica comum para esconder vírus e outro malware é a de incorporá-los em arquivos compostos, como arquivos ou bancos de dados de e-mail. Para detectar vírus e outro tipo de malware que estão ocultos dessa forma, é necessário descompactar os arquivos compostos, o que pode reduzir a velocidade da verificação. É possível restringir o modo de verificação dos arquivos compostos, o que aumentará a velocidade desta.

O método usado para processar um arquivo composto infectado (desinfecção ou exclusão) depende do tipo do arquivo.

O Antivírus de Arquivos desinfeta arquivos compostos nos formatos RAR, ARJ, ZIP, CAB e LHA e excluir arquivos em todos outros formatos (exceto bancos de dados de e-mail).

Para configurar a verificação de arquivos compostos:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de Arquivos**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de Arquivos.

3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   A janela **Antivírus de Arquivos** abre.

4. Na janela **Antivírus de Arquivos**, selecione a guia **Desempenho**.

5. Na seção **Verificação de arquivos compostos**, especifique os tipos de arquivos compostos que deseja verificar: arquivos compactados, pacotes de instalação ou arquivos em formatos do Office.

6. Para verificar somente os arquivos compostos novos e modificados, selecione a caixa de seleção **Verificar somente arquivos novos e alterados**.

   O Antivírus de Arquivos somente verificará os arquivos compostos novos e modificados de todos os tipos.

7. Clique no botão **Adicional**.

   A janela **Arquivos compostos** é exibida.

8. Na seção **Verificação em segundo plano**, execute uma das seguintes ações:

   - Para bloquear que o Antivírus de Arquivos descompacte os arquivos compostos em segundo plano, desmarque a caixa de seleção **Descompactar arquivos compostos em segundo plano**.

- Para permitir que o Antivírus de Arquivos descompacte os arquivos compostos ao verificar em segundo plano, selecione a caixa de seleção **Descompactar arquivos compostos em segundo plano** e especifique o valor necessário no campo **Tamanho mínimo de arquivo**.

9. Na seção **Limite de tamanho**, execute uma das seguintes operações:

   - Para bloquear que o Antivírus de Arquivos descompacte os arquivos compostos, selecione a caixa de seleção **Não descompactar arquivos compostos grandes** e especifique o valor necessário no campo **Tamanho máximo de arquivo**. O Antivírus de Arquivos não descompactará arquivos compostos que são maiores do que o tamanho especificado.

   - Para permitir que o Antivírus de Arquivos descompacte grandes arquivos compostos, desmarque a caixa de seleção **Não descompactar arquivos compostos grandes**.

     O arquivo é considerado grande quando o tamanho dele excede o valor no campo **Tamanho máximo de arquivo**.

   O Antivírus de Arquivos verifica arquivos grandes que são extraídos de arquivos compactados, não importando se a caixa de seleção **Não descompactar arquivos compostos grandes** está marcada.

10. Clique em **OK**.

11. Na janela **Antivírus de Arquivos**, clique em **OK**.

12. Para salvar as alterações, clique no botão **Salvar**.

Alterar o modo de verificação

Modo de verificação refere-se às condições de execução do Antivírus de Arquivos para verificação de arquivos. Por padrão, o Kaspersky Endpoint Security realiza a verificação de arquivos no modo de inteligente. Neste modo de verificação, o Antivírus de Arquivos decide quando verifica, ou não, os arquivos, após analisar as operações com o arquivo executadas pelo usuário, por um aplicativo no lugar do usuário (usando a conta atualmente ativa ou uma conta de usuário diferente) ou pelo sistema operacional. Por exemplo, ao trabalhar com um documento do Microsoft Office Word, o Kaspersky Endpoint Security verifica o arquivo quando ele é aberto pela primeira vez e fechado pela última vez. O arquivo não é verificado durante as operações intermediárias de gravação.

Para alterar o modo de verificação dos arquivos:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de Arquivos**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de Arquivos.

3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   A janela **Antivírus de Arquivos** abre.

4. Na janela **Antivírus de Arquivos**, selecione a guia **Adicional**.

5. Na seção **Modo de verificação**, selecione o modo desejado:

   - **Modo inteligente**.

   - **Ao acessar e modificar**.

- **Ao acessar**.
- **Ao executar**.

6. Clique em **OK**.

7. Para salvar as alterações, clique no botão **Salvar**.

Proteção de e-mail. Antivírus de E-mail

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado com o Microsoft Windows para estações de trabalho. Este componente estará indisponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado no Microsoft Windows para servidores de arquivos.

Esta seção contém informações sobre o Antivírus de E-mail e as instruções para definir as configurações dos componentes.

Sobre o Antivírus de E-mail

O Antivírus de E-mail verifica mensagens de e-mail recebidas e enviadas para detectar vírus e outras ameaças. É iniciado juntamente com o Kaspersky Endpoint Security, permanece sempre na RAM do computador e verifica todas as mensagens que são enviadas ou recebidas via protocolos POP3, SMTP, IMAP, MAPI e NNTP. Se nenhuma ameaça for detectada na mensagem, ela ficará disponível para o usuário e/ou será processada.

Ao detectar uma ameaça em uma mensagem de e-mail, o Antivírus de E-mail executa as seguintes operações:

1. Identifica o tipo de objeto detectado na mensagem de e-mail (como um *Cavalo de troia*).
2. Uma mensagem de e-mail recebe um dos seguintes status:
    - *Provavelmente infectada*. Esse status é atribuído se a verificação não puder determinar se a mensagem de e-mail está definitivamente infectada. A mensagem de e-mail possivelmente contenha uma sequência de código, que é típico de vírus ou outro tipo de malware, ou código modificado de um vírus conhecido.
    - *Infectada*. Esse status é atribuído a um objeto se a verificação de uma mensagem de e-mail encontrar uma seção do código de um vírus conhecido que está incluído nos bancos de dados do Antivírus de Kaspersky Endpoint Security.
    - *Não encontrado*. Esse status é atribuído a um objeto se a verificação de uma mensagem de e-mail não detectar vírus ou outras ameaças.

Em seguida, o aplicativo bloqueia a mensagem de e-mail, exibe uma notificação sobre o objeto detectado (se isto for especificado nas configurações de notificação) e executa a ação especificada nas configurações do Antivírus de E-mail.

Este componente interage com os clientes de e-mail instalados no computador. Uma extensão integrada está disponível para o cliente de correio do Microsoft Office Outlook® e permite efetuar o controle detalhado das configurações da verificação de mensagem. A extensão do Antivírus de E-mail é incorporada no cliente de e-mail do Microsoft Office Outlook durante a instalação do Kaspersky Endpoint Security.

A operação do Antivírus de E-mail está representada pelo ícone do aplicativo na área de notificação da barra de tarefas. Quando o Antivírus de E-mail está verificando uma mensagem de e-mail, o ícone do aplicativo é alterado para  .

Ativar e desativar o Antivírus de E-mail

Por padrão, o Antivírus de E-mail está ativo e é executado no modo recomendado pelos especialistas da Kaspersky. Se necessário, você pode desativar o Antivírus de E-mail.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

Para ativar ou desativar o Antivírus de E-mail na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Proteção**.
   A seção **Proteção** é exibida.
4. Clique com o botão direito do mouse para abrir o menu de contexto da linha com as informações sobre o componente Antivírus de E-mail.
   Será aberto um menu para a seleção de ações.
5. Execute uma das seguintes ações:
   - Para ativar o Antivírus de E-mail, selecione **Iniciar** no menu.
     O ícone de status do componente , exibido à esquerda, na linha do **Antivírus de E-mail**, muda para o ícone .
   - Para desativar o Antivírus de E-mail, selecione **Interromper** no menu.
     O ícone de status do componente , exibido à esquerda, na linha do **Antivírus de E-mail**, muda para o ícone .

Para ativar ou desativar o Antivírus de E-mail na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de E-mail**.
   Na parte direita da janela, são exibidas as configurações do componente Antivírus de E-mail.
3. Execute uma das seguintes ações:
   - Se desejar ativar o Antivírus de E-mail, marque a caixa de seleção **Ativar Antivírus de E-mail**.
   - Se desejar desativar o Antivírus de E-mail, desmarque a caixa de seleção **Ativar Antivírus de E-mail**.
4. Para salvar as alterações, clique no botão **Salvar**.

Configurar o Antivírus de E-mail

As seguintes opções de configuração do Antivírus de E-mail estão disponíveis:

- Alterar o nível de segurança de e-mails.
  Selecione um dos níveis de segurança de e-mails predefinidos ou configure um nível de segurança personalizado.

A alteração das configurações do nível de segurança de e-mails não impede a reversão para o nível recomendado quando desejado.

- Alterar a ação do Kaspersky Endpoint Security ao detectar mensagens de e-mail infectadas.
- Editar o escopo de proteção do Antivírus de E-mail.
- Configurar a verificação de arquivos compostos em anexos das mensagens de e-mail.

  Você pode ativar ou desativar a verificação de anexos de mensagem, limitar o tamanho máximo de anexos de mensagem a verificar e limitar a duração de verificação de anexo de mensagem máxima.
- Configurar a filtragem pelo tipo de anexos de mensagem de e-mail.

  Filtrar anexos de mensagem por tipo permite a renomeação automática ou exclusão de arquivos dos tipos especificados.
- Configurar o Analisador Heurístico.

  Para aumentar a eficácia da proteção, você pode usar a análise heurística. Durante a análise heurística, o Kaspersky Endpoint Security analisa a atividade dos aplicativos no sistema operacional. A análise heurística consegue detectar ameaças em mensagens que ainda não foram registradas nos bancos de dados do Kaspersky Endpoint Security.
- Configurar a verificação de e-mail no Microsoft Office Outlook.

  Uma extensão incorporada está disponível para o cliente de correio do Microsoft Office Outlook, que permite configurações convenientes para verificação de e-mail.

  Trabalhando com outros clientes de e-mail, incluindo o Microsoft Outlook Express®, Windows Mail e Mozilla™ Thunderbird™, o componente de Antivírus de E-mail verifica o tráfego por meio dos protocolos SMTP, POP3, IMAP e NNTP.

  Trabalhando com o cliente de e-mail, Mozilla Thunderbird, o Antivírus de E-mail não verificará as mensagens que são transmitidas por meio do protocolo IMAP quanto a vírus e outras ameaças, se os filtros forem usados para mover mensagens da pasta **Entrada**.

Alterar o nível de segurança de e-mails

O Antivírus de E-mail emprega vários grupos de configurações para proteger o tráfego de e-mail. Estes grupos de configurações são chamados *níveis de segurança de e-mails*. Existem três níveis de segurança de e-mails: **Alto**, **Recomendado** e **Baixo**. O nível de segurança de arquivos **Recomendado** oferece as configurações ideais e recomendadas pela Kaspersky.

Para alterar o nível de segurança de e-mails predefinido:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de E-mail**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de E-mail.
3. Na seção **Nível de segurança**, execute uma das seguintes operações:

   - Se desejar executar um dos níveis de segurança de e-mails predefinidos (**Alto**, **Recomendado** ou **Baixo**), use a barra deslizante para selecionar o desejado.

- Se desejar configurar um nível de segurança de e-mails personalizado, clique no botão **Configurações** e especifique as configurações do **Antivírus de E-mail**.

  Após configurar um nível de segurança de e-mails personalizado, o nome do nível de segurança, na seção **Nível de segurança**, muda para **Personalizado**.

- Se desejar alterar o nível de segurança de e-mails para **Recomendado**, clique no botão **Padrão**.

4. Para salvar as alterações, clique no botão **Salvar**.

Alterar a ação a executar em mensagens de e-mail infectadas

Para alterar a ação a executar em mensagens de e-mail infectadas:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de E-mail**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de E-mail.
3. Na seção **Ação ao detectar ameaça**, selecione a ação do Kaspersky Endpoint Security ao detectar uma mensagem infectada:
   - **Selecionar ação automaticamente**.
   - **Executar ação: Desinfectar. Excluir se a desinfecção falhar**.
   - **Executar ação: Desinfectar.**
   - **Executar ação: Remover**.
   - **Executar ação: Bloquear**.
4. Para salvar as alterações, clique no botão **Salvar**.

Editar o escopo de proteção do Antivírus de E-mail

O escopo de proteção refere-se aos objetos que são verificados pelo componente quando está ativo. O escopo de proteção de componentes diferentes tem propriedades diversas. As propriedades do escopo de proteção do Antivírus de E-mail contêm as configurações da integração do Antivírus de E-mail em clientes de e-mail, e o tipo de mensagens de e-mail e os protocolos de e-mail cujo tráfego é verificado pelo Antivírus de E-mail. Por padrão, o Kaspersky Endpoint Security verifica as mensagens e o tráfego de e-mail recebidos e enviados por meio de protocolos POP3, SMTP, NNTP e IMAP, e está incorporado ao cliente de e-mail do Microsoft Office Outlook.

Para criar o escopo de proteção do Antivírus de E-mail:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de E-mail**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de E-mail.

3. Clique no botão **Configurações**.

   A janela **Antivírus de E-mail** é exibida.

4. Selecione a guia **Geral**.

5. Na seção **Escopo de proteção**, execute uma das seguintes operações:

   - Se desejar que o Antivírus de E-mail verifique todas as mensagens de e-mail recebidas e enviadas em seu computador, selecione a opção **Mensagens enviadas e recebidas**.
   - Se desejar que o Antivírus de E-mail verifique apenas as mensagens recebidas em seu computador, selecione a opção **Apenas mensagens recebidas**.

     Se você escolher verificar apenas as mensagens recebidas, recomenda-se executar uma verificação única de todas as mensagens de saída porque há uma possibilidade de que o seu computador tenha worms de e-mail que estão se espalhando por e-mail. Esta ação é necessária para evitar problemas resultantes do envio de mensagens de e-mail não monitoradas ou mensagens infectadas de seu computador.

6. Na seção **Conectividade**, execute o seguinte:

   - Se desejar que o Antivírus de E-mail verifique as mensagens que são transmitidas através dos protocolos POP3, SMTP, NNTP e IMAP antes de chegarem ao computador, marque a caixa de seleção **Tráfego POP3 / SMTP / NNTP / IMAP**.

     Se não desejar que o Antivírus de E-mail verifique as mensagens que são transmitidas através dos protocolos POP3, SMTP, NNTP, IMAP e MAPI antes de chegarem ao computador, desmarque a caixa de seleção **Tráfego POP3 / SMTP / NNTP / IMAP**. Nesse caso, as mensagens serão verificadas pela extensão do Antivírus de E-mail incorporada no cliente de correio do Microsoft Office Outlook depois que elas são recebidas no computador do usuário se a caixa de seleção **Adicional: Extensão do Microsoft Office Outlook** estiver selecionada.

     Se você usar um cliente de e-mail que não seja o Microsoft Office Outlook, as mensagens de e-mail transmitidas através dos protocolos POP3, SMTP, NNTP e IMAP não serão verificadas pelo Antivírus de E-mail quando a caixa de seleção **Tráfego POP3 / SMTP / NNTP /IMAP** estiver desmarcada.

   - Se desejar permitir o acesso às configurações do Antivírus de E-mail a partir do Microsoft Office Outlook e ativar a verificação de mensagens transmitidas através dos protocolos POP3, SMTP, NNTP, IMAP e MAPI, após chegarem ao computador usando uma extensão incorporada no Microsoft Office Outlook, marque a caixa de seleção **Adicional: Extensão do Microsoft Office Outlook**.

     Se desejar bloquear o acesso às configurações do Antivírus de E-mail a partir do Microsoft Office Outlook e desativar a verificação de mensagens transmitidas através dos protocolos POP3, SMTP, NNTP, IMAP e MAPI, após elas chegarem ao computador usando uma extensão incorporada no Microsoft Office Outlook, desmarque a caixa de seleção **Adicional: Extensão do Microsoft Office Outlook**.

     A extensão do Antivírus de E-mail é incorporada no cliente de e-mail do Microsoft Office Outlook durante a instalação do Kaspersky Endpoint Security.

7. Clique em **OK**.

8. Para salvar as alterações, clique no botão **Salvar**.

Verificar arquivos compostos anexados a mensagens de e-mail

Para configurar a verificação de arquivos compostos anexados às mensagens de e-mail:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de E-mail**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de E-mail.
3. Clique no botão **Configurações**.

   A janela **Antivírus de E-mail** é exibida.
4. Selecione a guia **Geral**.
5. Execute o seguinte na seção **Verificação de arquivos compostos**:

   - Se desejar que o Antivírus de E-mail ignore os arquivos anexados às mensagens, desmarque a caixa de seleção **Verificar arquivos compactados anexados**.
   - Se desejar que o Antivírus de E-mail ignore anexos de mensagens com mais de N megabytes, marque a caixa de seleção **Não verificar arquivos compactados com mais de N MB**. Se marcar esta caixa de seleção, especifique o tamanho máximo do arquivo compactado no campo ao lado do nome da caixa de seleção.
   - Se desejar que o Antivírus de E-mail verifique anexos de mensagens que demoram mais de N segundos a serem verificados, desmarque a caixa de seleção **Não verificar arquivos compactados há mais de** N seg.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Filtrar anexos em mensagens de e-mail

Os programas maliciosos podem ser distribuídos na forma de anexos em mensagens de e-mail. Você pode configurar a filtragem baseada no tipo de anexos da mensagem para que os arquivos dos tipos especificados sejam automaticamente renomeados ou excluídos. Ao renomear um anexo de um determinado tipo, o Kaspersky Endpoint Security pode proteger seu computador contra a execução automática de um programa malicioso.

Para configurar a filtragem de anexos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de E-mail**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de E-mail.
3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   A janela **Antivírus de E-mail** é exibida.
4. Na janela **Antivírus de E-mail**, selecione a guia **Filtro de anexos**.

5. Execute uma das seguintes ações:

- Se não desejar usar o Antivírus de E-mail para filtrar anexos de mensagens, selecione a opção **Desativar a filtragem**.
- Se desejar que o Antivírus de E-mail renomeie os anexos de mensagens dos **tipos especificados**, selecione a opção **Renomear tipos de anexos especificados**.

Observe que o formato real de um arquivo pode não combinar com a extensão do nome do arquivo.

Se você ativar a filtragem de objetos que são anexados a mensagens de e-mail, o Antivírus de E-mail poderá renomear ou excluir os arquivos com as seguintes extensões:

com – arquivo executável de um aplicativo de até 64 KB

exe – arquivo executável ou arquivo autoextraível

sys – arquivo do sistema Microsoft Windows

prg – texto de programa Base™, Clipper ou Microsoft Visual FoxPro® ou um programa WAVmaker

bin – arquivo binário

bat – arquivo em lote

cmd – arquivo de comando do Microsoft Windows NT (semelhante a um arquivo bat do DOS), SO/2

dpl – biblioteca Borland Delphi compactada

dll – biblioteca de link dinâmica

scr – tela de início do Microsoft Windows

cpl – módulo do painel de controle do Microsoft Windows

ocx – objeto Microsoft OLE (Vinculação e Incorporação de Objeto)

tsp – programa que executa em modo de tempo parcial

drv – driver de dispositivo

vxd – driver de dispositivo virtual do Microsoft Windows

pif – arquivo de informações de programa

lnk – arquivo de link do Microsoft Windows

reg – arquivo da chave de registro do sistema do Microsoft Windows

ini – arquivo de configuração que contém dados de configuração do Microsoft Windows, do Windows NT e de alguns aplicativos

cla – classe de Java

vbs – script do Visual Basic®

vbe – extensão de vídeo de BIOS

js, jse – texto de fonte de JavaScript

htm – documento de hipertexto

htt – cabeçalho de hipertexto do Microsoft Windows

hta – programa de hipertexto do Microsoft Internet Explorer®

asp – script de Páginas do Servidor Ativo

chm – arquivo HTML compilado

pht – arquivo HTML com scripts PHP integrados

php – script integrado em arquivos HTML

wsh – arquivo do Microsoft Windows Script Host

wsf – script do Microsoft Windows

the – arquivo de papel de parede da área de trabalho do Microsoft Windows 95

hlp – arquivo Win Help

eml – mensagem do Microsoft Outlook Express

nws – nova mensagem de e-mail do Microsoft Outlook Express

msg – mensagem de e-mail do Microsoft Mail

plg – mensagem de e-mail

mbx – extensão de e-mails salvos do Microsoft Office Outlook

doc* – documentos do Microsoft Office Word, como: doc para documentos do Microsoft Office Word, docx para documentos do Microsoft Office Word 2007 com suporte a XML e docm para documentos do Microsoft Office Word 2007 com suporte a macros

dot* – modelos de documento do Microsoft Office Word, como: dot para modelos de documento do Microsoft Office Word, dotx para modelos de documento do Microsoft Office Word 2007, dotm para modelos de documento do Microsoft Office Word 2007 com suporte a macros

fpm – programa de banco de dados, arquivo de início do Microsoft Visual FoxPro

rtf – documento de Formato Rich Text

shs – fragmento do manipulador de objeto do Windows Shell Scrap

dwg – banco de dados de desenho do AutoCAD®

msi – pacote do Microsoft Windows Installer

otm – projeto VBA para Microsoft Office Outlook

pdf – documento do Adobe Acrobat

swf – objeto de pacote do Shockwave® Flash

jpg, jpeg – formato gráfico de imagem compactada

emf – arquivo de formato de Metarquivo Aprimorado. Próxima geração de metarquivos do SO do Microsoft Windows. Os arquivos EMF não são suportados pelo Microsoft Windows de 16 bits.

ico – arquivo de ícone de objeto

ov? – arquivos executáveis do Microsoft Office Word

xl* – documentos e arquivos do Microsoft Office Excel, como: xla, a extensão para Microsoft Office Excel, xlc para diagramas, xlt para modelos de documento, xlsx para pastas de trabalho do Microsoft Office Excel 2007, xltm para pastas de trabalho do Microsoft Office Excel 2007 com suporte de macros, xlsb para pastas de trabalho do Microsoft Office Excel 2007 em formato binário (não XML), xltx para modelos do Microsoft Office Excel 2007, xlsm para modelos do Microsoft Office Excel 2007 com suporte de macros e xlam para plug-ins do Microsoft Office Excel 2007 com suporte de macros

pp* – documentos e arquivos do Microsoft Office PowerPoint®, como: pps para slides do Microsoft Office PowerPoint, ppt para apresentações, pptx para apresentações do Microsoft Office PowerPoint 2007, pptm para apresentações do Microsoft Office PowerPoint 2007 com suporte de macros, potx para modelos de apresentação do Microsoft Office PowerPoint 2007, potm para modelos de apresentação do Microsoft Office PowerPoint 2007 com suporte de macros, ppsx para apresentações de slides do Microsoft Office PowerPoint 2007, ppsm para apresentações de slides do Microsoft Office PowerPoint 2007 com suporte de macros e ppam para plug-ins do Microsoft Office PowerPoint 2007 com suporte de macros

md* – documentos e arquivos do Microsoft Office Access®, como: mda para grupos de trabalho do Microsoft Office Access e mdb para bancos de dados

sldx – um slide do Microsoft PowerPoint 2007

sldm – um slide do Microsoft PowerPoint 2007 com suporte a macros

thmx – um tema do Microsoft Office 2007

- Se desejar que o Antivírus de E-mail exclua os anexos de mensagens dos tipos especificados, selecione a opção **Excluir tipos de anexos especificados**.

6. Se você tiver selecionado a opção **Renomear tipos de anexos especificados** ou a opção **Excluir tipos de anexos especificados** na etapa anterior, selecione as caixas em frente dos tipos relevantes de arquivos.

   A lista de tipos de arquivos pode ser alterada usando os botões **Adicionar**, **Editar** e **Remover**.

7. Clique em **OK**.

8. Para salvar as alterações, clique no botão **Salvar**.

Verificar e-mails no Microsoft Office Outlook

Durante a instalação do Kaspersky Endpoint Security, a extensão do Antivírus de E-mail é integrada no Microsoft Office Outlook (daqui em diante também referido como Outlook). Isso permite abrir as configurações do Antivírus de E-mail internamente no Outlook e especificar o momento da verificação das mensagens de e-mail para detectar vírus e outras ameaças. A extensão do Antivírus de E-mail para Outlook consegue verificar mensagens recebidas e enviadas que são transmitidas via protocolos POP3, SMTP, NNTP, IMAP e MAPI.

As configurações do Antivírus de E-mail podem ser definidas diretamente no Outlook se a caixa de seleção **Adicional: extensão do Microsoft Office Outlook** estiver marcada na interface do Kaspersky Endpoint Security.

No Outlook, as mensagens recebidas são verificadas primeiro pelo Antivírus de E-mail (se a caixa de seleção **Tráfego de POP3 / SMTP / NNTP / IMAP** estiver marcada na interface do Kaspersky Endpoint Security) e, em seguida, pela extensão do Antivírus de E-mail para Outlook. Se o Antivírus de E-mail detectar um objeto malicioso em uma mensagem, você será alertado sobre esse evento.

A ação a executar na janela de notificação determina o componente que eliminará a ameaça na mensagem de e-mail: Antivírus de E-mail ou plug-in do Antivírus de E-mail para Outlook.

- Se selecionar **Desinfectar** ou **Remover** na janela de notificação, a eliminação da ameaça será executada pelo Antivírus de E-mail.
- Se você selecionar **Ignorar** na janela de notificação ao usuário, a extensão do Antivírus de E-mail para Outlook eliminará a ameaça.

As mensagens enviadas são verificadas primeiramente pela extensão do Antivírus de E-mail para Outlook e, em seguida, pelo Antivírus de E-mail.

Configurar verificação de e-mails no Outlook

Para configurar a verificação de e-mail no Outlook 2007:

1. Abra a janela principal do Outlook 2007.
2. Selecione **Serviço** → **Configurações** da barra de menus.

   A janela **Opções** abre.
3. Na janela **Opções**, selecione a guia **Proteção de e-mail**.

Para configurar a verificação de e-mail no Outlook 2010/2013:

1. Abra a janela principal do Outlook.

   Selecione a guia **Arquivo** no canto esquerdo superior.
2. Clique no botão **Opções**.

   A janela **Opções do Outlook** é aberta.
3. Selecione a seção **Suplementos**.

As configurações de plug-ins incorporadas ao Outlook são exibidas na parte direita da janela.

4. Clique no botão **Opções de suplementos**.

Configurar verificação de correio usando o Kaspersky Security Center

Se o correio for verificado usando a extensão do Antivírus de E-mail para Outlook, recomenda-se usar o Modo Cache do Exchange. Para obter informações mais detalhadas sobre o modo Cache do Exchange e recomendações sobre seu uso, consulte a Base de Dados de Conhecimento da Microsoft: https://technet.microsoft.com/pt-br/library/cc179175.aspx.

Para configurar o modo operacional da extensão do Antivírus de E-mail para Outlook usando o Kaspersky Security Center:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja configurar a verificação de correio.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Proteção antivírus**, selecione a subseção **Antivírus de E-mail**.
7. Na seção **Nível de segurança**, clique no botão **Configurações**.

   A janela **Antivírus de E-mail** é exibida.
8. Na seção **Conectividade**, clique no botão **Configurações**.

   A janela **Proteção de e-mail** é exibida.
9. Na janela **Proteção de e-mail**:
   - Marque a caixa de seleção **Verificar ao receber** se desejar que a extensão do Antivírus de E-mail para Outlook verifique mensagens de entrada quando elas chegam à caixa do correio.
   - Marque a caixa de seleção **Verificar ao ler** se desejar que a extensão do Antivírus de E-mail para Outlook verifique mensagens de entrada no momento em que o usuário as abre.
   - Marque a caixa de seleção **Verificar ao enviar** se desejar que a extensão do Antivírus de E-mail para Outlook verifique mensagens de saída quando elas são enviadas.
10. Na janela **Proteção de e-mail**, clique em **OK**.

11. Na janela **Antivírus de E-mail**, clique em **OK**.

12. Aplique a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Proteção do computador na Internet. Antivírus da Web

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado com o Microsoft Windows para estações de trabalho. Este componente estará indisponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado no Microsoft Windows para servidores de arquivos.

Esta seção contém informações sobre o Antivírus da Web e as instruções para definir as configurações do componente.

Sobre o Antivírus da Web

Sempre que você usa a Internet, as informações armazenadas no computador ficam expostas à infecção por vírus e outro tipo de malware. Eles podem se infiltrar no computador enquanto o usuário baixa algum software gratuito ou navega por sites sujeitos a ataques de criminosos. Os worms de rede podem invadir o computador no momento em que você se conectar à Internet, mesmo sem abrir uma página da Web ou baixar um arquivo.

O Antivírus da Web oferece proteção ao computador durante a entrada e a saída de dados pelos protocolos HTTP e FTP, e verifica a existência dos URLs na lista de endereços da Web maliciosos e de phishing.

O Antivírus da Web intercepta e analisa toda página da Web ou arquivo, para detectar vírus ou outras ameaças, acessados por usuário ou aplicativo através dos protocolos HTTP ou FTP. Em seguida, o que acontece:

- O usuário obtém acesso imediato à página ou ao arquivo quando estes não contêm código malicioso.
- Se um usuário acessar uma página da Web ou arquivo que contenha o código malicioso, o aplicativo executará a ação especificada nas configurações de Antivírus da Web.

Ativar e desativar o Antivírus da Web

Por padrão, o Antivírus da Web está ativo e é executado no modo recomendado pelos especialistas da Kaspersky. Se necessário, você pode desativar o Antivírus da Web.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

Para ativar ou desativar o Antivírus da Web na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Proteção**.

   A seção **Proteção** é exibida.

4. Clique com o botão direito do mouse para abrir o menu de contexto da linha com as informações sobre o componente Antivírus da Web.

   Será aberto um menu para a seleção de ações.

5. Execute uma das seguintes ações:

   - Para ativar o Antivírus da Web, selecione **Iniciar** no menu.

     O ícone de status do componente , exibido à esquerda na linha do **Antivírus da Web**, muda para o ícone .

   - Para desativar o Antivírus da Web, selecione **Interromper** no menu.

     O ícone de status do componente , exibido à esquerda na linha do **Antivírus da Web**, muda para o ícone .

Para ativar ou desativar o Antivírus da Web na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus da Web**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus da Web.

3. Execute uma das seguintes ações:

   - Se desejar ativar o Antivírus da Web, marque a caixa de seleção **Ativar Antivírus da Web**.
   - Se desejar desativar o Antivírus da Web, desmarque a caixa de seleção **Ativar Antivírus da Web**.

4. Para salvar as alterações, clique no botão **Salvar**.

Configurar o Antivírus da Web

As seguintes opções de configuração do Antivírus da Web estão disponíveis:

- Alterar o nível de segurança de tráfego da Web.

  Você pode selecionar um dos níveis de segurança de tráfego da Web predefinidos que é recebido e transmitido através dos protocolos HTTP e FTP, ou configurar um nível de segurança de tráfego da Web personalizado.

  A alteração das configurações do nível de segurança do nível de segurança de tráfego da Web não impede a reversão para o nível recomendado quando desejado.

- Alterar a ação do Kaspersky Endpoint Security ao detectar objetos maliciosos no tráfego da Web.

  Quando a análise de um objeto HTTP mostrar que ele contém um código malicioso, a ação do componente Antivírus da Web dependerá do que você tiver especificado.

- Configurar a verificação de links em bancos de dados de URLs maliciosos e de phishing no Antivírus da Web.
- Configurar a análise heurística ao executar ao verificar o tráfego da Web para detectar programas maliciosos.

  Para aumentar a eficácia da proteção, você pode usar a análise heurística. Durante a análise heurística, o Kaspersky Endpoint Security analisa a atividade dos aplicativos no sistema operacional. A análise heurística consegue detectar ameaças que ainda não tenham registros nos bancos de dados do Kaspersky Endpoint Security.

- Configurar a análise heurística ao verificar páginas da Web para detectar links de phishing.

- Otimizar a verificação no Antivírus da Web de tráfego da Web que é enviado e recebido através dos protocolos HTTP e FTP.

- Criar uma lista de URLs confiáveis.

  Você pode criar uma lista de URLs em cujo conteúdo confia. O Antivírus da Web não analisa as informações sobre URLs confiáveis para detectar vírus ou outros tipos de ameaças. Esta opção pode ser útil, por exemplo, quando o Antivírus da Web interferir no download de um arquivo de um site conhecido.

  O URL refere-se ao endereço de uma página ou site determinado.

Alterar o nível de segurança de tráfego da Web

O Antivírus da Web emprega vários grupos de configurações para proteger os dados que são recebidos e transmitidos através dos protocolos HTTP e FTP. Estes grupos de configurações são chamados *níveis de segurança de tráfego da Web*. Existem três níveis de segurança de tráfego da Web predefinidos: **Alto**, **Recomendado** e **Baixo**. O nível de segurança de tráfego da Web **Recomendado** oferece o grupo de configurações ideal e recomendado pela Kaspersky.

Para alterar o nível de segurança de tráfego da web:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus da Web**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus da Web.
3. Na seção **Nível de segurança**, execute uma das seguintes operações:

   - Se desejar executar um dos níveis de segurança de tráfego da Web predefinidos (**Alto**, **Recomendado** ou **Baixo**), use a barra deslizante para selecionar o desejado.
   - Se desejar configurar um nível de segurança de tráfego da Web personalizado, clique no botão **Configurações** e especifique as configurações do **Antivírus da Web**.

     Após configurar um nível de segurança de tráfego da Web personalizado, o nome do nível de segurança, na seção **Nível de segurança**, muda para **Personalizado**.
   - Se desejar alterar o nível de segurança de tráfego da Web para **Recomendado**, clique no botão **Padrão**.
4. Para salvar as alterações, clique no botão **Salvar**.

Alterar a ação a executar em objetos maliciosos no tráfego da Web

Para alterar a ação a executar em objetos maliciosos no tráfego da Web:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus da Web**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus da Web.

3. Na seção **Ação ao detectar ameaça**, selecione ação do Kaspersky Endpoint Security ao detectar objetos maliciosos no tráfego da Web:

   - **Selecionar ação automaticamente**.
   - **Bloquear download**.
   - **Permitir download**.

4. Para salvar as alterações, clique no botão **Salvar**.

Verificar URLs em bancos de dados de URLs maliciosos e de phishing no Antivírus da Web

Ao verificar se links estão incluídos na lista de endereços de phishing da Internet, evita-se *ataques de phishing*. O ataque de phishing se disfarça, por exemplo, como uma mensagem de e-mail que é enviada pelo seu banco, e que contém um link para o site oficial da instituição. Ao clicar no link, você é direcionado para uma cópia exata do site do banco e pode até ver o endereço real no navegador, embora, na verdade, esteja em um site falso. Desse momento em diante, todas as suas ações no site são rastreadas e podem ser usadas para roubá-lo.

Como os links para sites de phishing podem ser recebidos de outras fontes além dos e-mails, como mensagens do ICQ, o Antivírus da Web monitora as tentativas de acessar um site de phishing no nível do tráfego da Web e bloqueia o acesso a esses locais. O kit de distribuição do Kaspersky Endpoint Security contém as listas de URLs de phishing.

Para configurar que o Antivírus da Web verifique os URLs nos bancos de dados de endereços maliciosos e de phishing:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus da Web**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus da Web.

3. Clique no botão **Configurações**.

   A janela **Antivírus da Web** é exibida.

4. Na janela **Antivírus da Web**, selecione a guia **Geral**.
5. Faça o seguinte:

   - Se desejar que o Antivírus da Web verifique se os URLs estão nos bancos de dados de endereços maliciosos da Web, na seção **Métodos de verificação**, marque a caixa de seleção **Verificar se os links estão listados no banco de dados de links maliciosos**.
   - Se desejar que o Antivírus da Web verifique se os URLs estão nos bancos de dados de endereços da Web de phishing, na seção **Configurações Antiphishing**, marque a caixa de seleção **Verificar se os links estão listados no banco de dados de links de phishing**.

   Você também pode verificar os links em relação a bancos de dados de reputação do Kaspersky Security Network.

6. Clique em **OK**.

7. Para salvar as alterações, clique no botão **Salvar**.

Usar o Analisador Heurístico com o Antivírus da Web

Para configurar a análise heurística:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus da Web**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus da Web.

3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   A janela **Antivírus da Web** é exibida.

4. Selecione a guia **Geral**.

5. Se desejar que o Antivírus da Web utilize a análise heurística para verificar o tráfego da Web a fim de detectar vírus ou outros malwares, na seção **Métodos de verificação**, marque a caixa de seleção **Análise heurística para detectar vírus** e use a barra deslizante para definir o nível da análise heurística: **verificação Superficial**, **verificação média** ou **verificação profunda**.

6. Se desejar que o Antivírus da Web use a análise heurística para verificar páginas da Web de links de phishing, na seção **Configurações Antiphishing**, marque a caixa de seleção **Análise heurística para detecção de links de phishing**.

7. Clique em **OK**.

8. Para salvar as alterações, clique no botão **Salvar**.

Editar a lista de URLs confiáveis

Para criar uma lista de URLs confiáveis:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus da Web**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus da Web.

3. Clique no botão **Configurações**.

   A janela **Antivírus da Web** é exibida.

4. Selecione a guia **URLs confiáveis**.

5. Marque a caixa de seleção **Não verificar tráfego da Web de URLs confiáveis**.

6. Crie uma lista de URLs/páginas em cujo conteúdo você confia. Para criar uma lista:

a. Clique no botão **Adicionar**.

A janela **Endereço Web/máscara de endereço Web** é aberta.

b. Insira o endereço do site/página ou máscara de endereço do site/página.

c. Clique em **OK**.

Aparece um novo registro na lista de URLs confiáveis.

7. Clique em **OK**.

8. Para salvar as alterações, clique no botão **Salvar**.

Proteção do tráfego do cliente de MI. Antivírus de MI

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado com o Microsoft Windows para estações de trabalho. Este componente estará indisponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado no Microsoft Windows para servidores de arquivos.

Esta seção contém informações sobre o Antivírus de MI e as instruções para definir as configurações do componente.

Sobre o Antivírus de MI

O Antivírus de MI verifica o tráfego de clientes de mensagens instantâneas (conhecidos como *clientes de MI)*.

Os Antivírus de MI não verificam mensagens transmitidas via canais criptografados.

As mensagens enviadas pelos cliente de MI talvez contenham os seguintes tipos de ameaças à segurança:

- URLs que tentam baixar um programa malicioso no computador
- URLs que direcionam a programas maliciosos e sites que são utilizados pelos invasores para ataques de phishing

  Os ataques de phishing visam roubar dados pessoais dos usuários, como números de cartão do banco, dados do passaporte, senhas dos sistemas de pagamento bancário e outros serviços on-line (como em sites de redes sociais ou contas de e-mail).

É possível aos clientes de MI realizar a transmissão de arquivos. Em tentativas de salvar tais arquivos, os arquivos são verificados pelo componente Antivírus de Arquivos.

O Antivírus de MI intercepta todas as mensagens enviadas ou recebidas pelo usuário por meio de um cliente de MI e as verifica para detectar links que ameacem a segurança do computador:

- Se nenhum URL perigoso for detectado na mensagem, ela ficará disponível para o usuário.
- Se forem detectados links perigosos em uma mensagem, o Antivírus de MI substitui a mensagem pelas informações sobre a ameaça na janela de mensagem do cliente de MI ativo.

Ativar e desativar Antivírus de MI

Por padrão, o Antivírus de MI está ativado e é executado no modo recomendado pelos especialistas da Kaspersky. Se necessário, é possível desativar o Antivírus de MI.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo

- Na janela de configurações do aplicativo

Para ativar ou desativar o Antivírus de MI na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Proteção**.

   A seção **Proteção** é exibida.
4. Clique com o botão direito do mouse na linha do **Antivírus de MI** para exibir o menu de contexto das ações do componente.
5. Execute uma das seguintes ações:

   - Para ativar o Antivírus de MI, selecione **Iniciar** no menu de contexto.

     O ícone de status do componente , exibido à esquerda na linha do **Antivírus de MI**, muda para o ícone .
   - Para desativar o Antivírus de MI, selecione **Interromper** no menu de contexto.

     O ícone de status do componente , exibido à esquerda na linha do **Antivírus de MI**, muda para o ícone .

Para ativar ou desativar o Antivírus de MI na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de MI**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de MI.
3. Execute uma das seguintes ações:

   - Se desejar ativar o Antivírus de MI, marque a caixa de seleção **Ativar o Antivírus de MI**.
   - Se desejar desativar o Antivírus de MI, desmarque a caixa de seleção **Ativar o Antivírus de MI**.
4. Para salvar as alterações, clique no botão **Salvar**.

Configurar o Antivírus de MI

Você pode executar as seguintes ações para configurar o Antivírus de MI:

- Configurar o escopo de proteção.

  Você pode expandir ou restringir o escopo de proteção alterando o tipo de mensagens do cliente de MI que é verificado.
- Configure a verificação de Antivírus de MI de links em mensagens de clientes de MI em relação a bancos de dados de endereços da Web de phishing e maliciosos.

Criar o escopo de proteção do Antivírus de MI

O escopo de proteção refere-se aos objetos que o componente verifica quando está ativado. O escopo de proteção de componentes diferentes tem propriedades diversas. O tipo de mensagens do cliente de MI, recebidas e enviadas, é uma propriedade do escopo de proteção do Antivírus de MI. Por padrão, o Antivírus de MI verifica os e-mails enviados e recebidos. Se desejar, você pode desativar a verificação do tráfego de saída.

Para criar o escopo de proteção:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de MI**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de MI.
3. Na seção **Escopo de proteção**, execute uma das seguintes operações:

   - Se desejar que o Antivírus de MI verifique todas as mensagens recebidas e enviadas de clientes de MI, selecione a opção **Mensagens enviadas e recebidas**.
   - Se desejar que o Antivírus de MI verifique apenas as mensagens recebidas de clientes de MI, selecione a opção **Apenas mensagens recebidas**.
4. Para salvar as alterações, clique no botão **Salvar**.

Verificar URLs em bancos de dados de URLs maliciosos e de phishing com o Antivírus de MI

Para configurar o Antivírus de MI para verificar URLs em relação a bancos de dados de endereços maliciosos e de phishing:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Antivírus de MI**.

   Na parte direita da janela, são exibidas as configurações do componente Antivírus de MI.
3. Na seção **Métodos de verificação**, selecione os métodos de verificação do Antivírus de MI:

   - Se desejar verificar se os links nas mensagens dos clientes de MI estão nos bancos de dados de endereços da Web maliciosos, marque a caixa de seleção **Verificar se os links estão listados no banco de dados de links maliciosos**.
   - Se desejar verificar links em mensagens do cliente de MI em relação ao banco de dados de endereços Web de phishing, marque a caixa de seleção **Verificar se os links estão listados no banco de dados de links de phishing**.
4. Para salvar as alterações, clique no botão **Salvar**.

Inspetor do Sistema

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado com o Microsoft Windows para estações de trabalho. Este componente estará indisponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado no Microsoft Windows para servidores de arquivos.

Esta seção contém as informações sobre o Inspetor do Sistema e as instruções para definir as configurações do componente.

Sobre o Inspetor do Sistema

O Inspetor do Sistema coleta informações sobre as ações de aplicativos no computador e as repassa a outros componentes com o objetivo de garantir uma proteção confiável.

Padrões de atividades perigosas (BSS)

Os Padrões de atividades perigosas (BSS) contêm sequências de ações de aplicativos que o Kaspersky Endpoint Security classifica com perigosas. Se a atividade de um aplicativo corresponder a um padrão de atividades perigosas, o Kaspersky Endpoint Security executará a ação especificada. A funcionalidade do Kaspersky Endpoint Security com base em padrões de atividades perigosas fornece Defesa Proativa ao computador.

Por padrão, se a atividade do aplicativo combina com uma assinatura de fluxo de comportamento, o Inspetor do sistema move o arquivo executável daquele aplicativo para a Quarentena.

Reverter as ações de malware

Com base nas informações coletadas pelo Inspetor do Sistema, o Kaspersky Endpoint Security pode **reverter ações realizadas pelo malware no sistema operacional** enquanto realiza a desinfecção.

Revertendo a atividade de malware no sistema operacional, o Kaspersky Endpoint Security toma medidas nos seguintes tipos da atividade de malware:

- Atividade de arquivo.

  O Kaspersky Endpoint Security exclui arquivos executáveis que foram criados por um programa malicioso e localizados em qualquer mídia, exceto de rede.

  O Kaspersky Endpoint Security exclui arquivos executáveis que foram criados por um programa no qual um programa malicioso penetrou.

  O Kaspersky Endpoint Security não restaura arquivos modificados ou apagados.

- Atividade de registro.

  O Kaspersky Endpoint Security exclui partições e chaves do registro que foram criadas pelo malware.

  O Kaspersky Endpoint Security não restaura partições modificadas ou apagadas e chaves do registro.

- Atividade de sistema.

  O Kaspersky Endpoint Security termina processos que foram iniciados por um programa malicioso.

  O Kaspersky Endpoint Security termina processos nos quais um programa malicioso penetrou.

  O Kaspersky Endpoint Security não reinicia processos que foram pausados por um programa malicioso.

- Atividade de rede.

  O Kaspersky Endpoint Security bloqueia a atividade de rede de programas maliciosos.

  O Kaspersky Endpoint Security bloqueia a atividade de rede de processos nos quais um programa malicioso penetrou.

A reversão de ações de malware pode ser iniciada pelo Antivírus de Arquivos ou durante uma verificação de vírus.

O procedimento de reverter operações de malware afeta um conjunto de dados definido rigidamente. A reversão não possui efeitos adversos sobre o sistema operacional ou sobre a integridade dos dados do computador.

Ativar e desativar o Inspetor do Sistema

Por padrão, o Inspetor do Sistema é ativado e é executado no modo recomendado pela Kaspersky. É possível desativar o Inspetor do Sistema, se necessário.

Não é recomendado desativar o Inspetor do Sistema a menos que seja absolutamente necessário, pois isso afetará o desempenho dos componentes de proteção. Os componentes de proteção podem solicitar dados coletados pelo Inspetor do Sistema para identificar uma ameaça detectada com maior precisão.

Existem duas maneiras para ativar e desativar o Inspetor do Sistema:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

*Para ativar ou desativar o Inspetor do Sistema na guia **Proteção e Controle** da janela principal do aplicativo:*

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Proteção**.

   A seção **Proteção** é exibida.
4. Clique com o botão direito do mouse para exibir o menu de contexto da linha com as informações sobre o componente Inspetor do Sistema.

   Será aberto um menu para a seleção de ações.
5. Execute uma das seguintes ações:

   - Para ativar o Inspetor do Sistema, selecione **Iniciar**.

     O ícone de status do componente , exibido à esquerda na linha do **Inspetor do Sistema**, muda para o ícone .
   - Para desativar o Inspetor do Sistema, selecione **Interromper**.

     O ícone de status do componente , exibido à esquerda na linha do **Inspetor do Sistema**, muda para o ícone .

Para ativar ou desativar o Inspetor do Sistema na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Inspetor do Sistema**.

   Na parte direita da janela, serão apresentadas as configurações do componente **Inspetor do Sistema**.
3. Execute uma das seguintes ações:

   - Para ativar o Inspetor do Sistema, marque a caixa de seleção **Ativar Inspetor do Sistema**.
   - Para desativar o Inspetor do Sistema, desmarque a caixa de seleção **Ativar Inspetor do Sistema**.
4. Para salvar as alterações, clique no botão **Salvar**.

Configurar o Inspetor do Sistema

Você pode executar as seguintes ações para configurar o Inspetor do Sistema:

- ativar ou desativar a proteção contra programas maliciosos;
- selecione a ação caso seja detectada uma atividade maliciosa em um programa;
- Ativar ou desativar a reversão de ações de malware durante a desinfecção.

Ativar ou desativar a proteção contra programas maliciosos

Para ativar ou desativar a proteção contra programas maliciosos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Inspetor do Sistema**.

   Na parte direita da janela, serão apresentadas as configurações do componente **Inspetor do Sistema**.
3. Execute uma das seguintes ações:

   - Marque a caixa de seleção **Ativar a prevenção contra exploração** se quiser que o Kaspersky Endpoint Security monitore arquivos utilizados por programas vulneráveis ao serem iniciados.

     Se o Kaspersky Endpoint Security detectar que um arquivo em uso por um programa vulnerável foi iniciado por outra pessoa que não seja o usuário, então ele atuará conforme a sua seleção na lista pop-up **Ação ao detectar ameaça**.

   - Marque a caixa de seleção **Ativar a prevenção contra exploração** se quiser que o Kaspersky Endpoint Security monitore arquivos utilizados por programas vulneráveis ao serem iniciados.
4. Para salvar as alterações, clique no botão **Salvar**.

Selecione a ação caso uma atividade maliciosa seja detectada em um programa

Para selecionar que fazer se um programa se envolver em atividade maliciosa, execute as seguintes etapas:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Inspetor do Sistema**.

   Na parte direita da janela, serão apresentadas as configurações do componente **Inspetor do Sistema**.
3. Na seção **Ação ao detectar ameaça** na lista pop-up **Ao detectar atividade de malware**, selecione a seguinte ação:

   - **Selecionar ação automaticamente**.
   - **Mover arquivo para a Quarentena**.
   - **Encerrar o programa malicioso**.
   - **Ignorar**.
4. Para salvar as alterações, clique no botão **Salvar**.

Ativar e desativar a reversão de ações de malware durante a desinfecção

Para ativar ou desativar a reversão das ações de malware durante a desinfecção:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Inspetor do Sistema**.

   Na parte direita da janela, serão apresentadas as configurações do componente **Inspetor do Sistema**.

3. Execute uma das seguintes ações:

- Para que o Kaspersky Endpoint Security reverta as ações de malware no sistema durante a desinfecção, marque a caixa de seleção **Reverter ações de malware durante a desinfecção**.

- Para que o Kaspersky Endpoint Security ignore as ações de malware no sistema durante a desinfecção, desmarque a caixa de seleção **Reverter ações de malware durante a desinfecção**.

4. Para salvar as alterações, clique no botão **Salvar**.

Firewall

Esta seção contém informações sobre o Firewall e as instruções para definir as configurações do componente.

Sobre o Firewall

Durante o uso da LAN e da Internet, o computador é exposto a vírus, outros tipos de malware e a vários ataques que exploram as vulnerabilidades dos sistemas operacionais e software.

O firewall protege os dados pessoais que estão armazenados no computador do usuário, bloqueando todos os tipos de ameaças ao sistema operacional quando o computador estiver conectado à Internet ou a uma rede local. O Firewall detecta todas as conexões de rede do computador do usuário e fornece uma lista de endereços IP, com indicação do status da conexão de rede padrão.

O componente Firewall filtra toda a atividade de rede segundo as regras de rede. A configuração de regras de rede permite especificar o nível pretendido de proteção do computador, desde bloquear o acesso à Internet de todos os aplicativos até permitir o acesso ilimitado.

Ativar ou desativar o Firewall

Por padrão, o Firewall está ativado e funciona no modo normal. É possível desativar o Firewall, se necessário.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

Para ativar ou desativar o Firewall na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Proteção**.
   A seção **Proteção** é exibida.
4. Clique com o botão direito do mouse na linha **Firewall** para abrir o menu de contexto de ações do Firewall.
5. Execute uma das seguintes ações:
   - Para ativar o Firewall, no menu de contexto, selecione **Iniciar**.
     O ícone de status do componente , exibido à esquerda na linha do **Firewall**, muda para o ícone .
   - Para desativar o Firewall, selecione **Interromper** no menu de contexto.
     O ícone de status do componente , exibido à esquerda na linha do **Firewall**, muda para o ícone .

Para ativar ou desativar o Firewall, na janela de configurações:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione **Firewall**.

   Na parte direita da janela, as configurações do componente Firewall são exibidas.

3. Execute uma das seguintes ações:

   - Para ativar o Firewall, marque a caixa de seleção **Ativar Firewall**.
   - Para desativar o Firewall, marque a caixa de seleção **Desativar Firewall**.

4. Para salvar as alterações, clique no botão **Salvar**.

Sobre as regras de rede

As *regras de rede* referem-se às ações executadas pelo Firewall que são permitidas ou bloqueadas ao detectar uma tentativa de conexão de rede.

O Firewall oferece proteção contra ataques à rede de diversos tipos e de dois níveis: nível de rede e nível de programa. A proteção no nível de rede é fornecida aplicando as regras de pacotes de rede. A proteção no nível de programa é empregada segundo as regras que permite o acesso dos aplicativos instalados aos recursos de rede.

Com base nos dois níveis de proteção do Firewall, é possível criar o seguinte:

- *Regras de pacotes de rede*. As regras de pacotes de rede impõem restrições a pacotes de rede, seja qual for o programa. Estas regras restringem o tráfego de rede de entrada e de saída através de portas específicas do protocolo de dados selecionado. O Firewall define determinadas regras de pacotes de rede por padrão.
- *Regras de rede de aplicativos*. As regras de rede de aplicativos impõem restrições à atividade de rede de um aplicativo específico. Elas têm em conta não só as características do pacote de rede, mas também o aplicativo específico para o qual este pacote de rede é direcionado ou que emitiu este pacote de rede. Estas regras possibilitam o ajuste da filtragem da atividade de rede: por exemplo, quando um determinado tipo de conexão de rede é bloqueado para alguns aplicativos, mas é permitido para outros.

As regras de pacotes de rede têm prioridade sobre as regras de rede dos aplicativos. Se ambas as regras de pacotes de rede e regras de rede dos aplicativos forem especificadas para o mesmo tipo de atividade de rede, esta é executada segundo as regras de pacotes de rede.

É possível especificar uma prioridade de execução para cada regra de pacotes de rede e para cada regra de rede dos aplicativos.

As regras de pacotes de rede têm prioridade sobre as regras de rede dos aplicativos. Se ambas as regras de pacotes de rede e regras de rede dos aplicativos forem especificadas para o mesmo tipo de atividade de rede, esta é executada segundo as regras de pacotes de rede.

As regras de rede para aplicativos funcionam da seguinte maneira: uma regra de rede para aplicativos inclui regras de acesso com base no status da rede: *pública, local* ou *confiável*. Por exemplo, os aplicativos no grupo de confiança de Alta restrição não têm nenhuma atividade de rede em redes de todos os status por padrão. Se uma regra de rede for especificada para um aplicativo individual (aplicativo pai), os processos filhos de outros aplicativos serão executados de acordo com a regra de rede do aplicativo pai. Se não houver regra de rede para o aplicativo, os processos filhos serão executados de acordo com a regra de acesso à rede do grupo de confiança do aplicativo.

Por exemplo, você proibiu todas as atividades de rede em redes de todos os status para todos os aplicativos, exceto o navegador X. Se você iniciar a instalação do navegador Y (processo filho) a partir do navegador X (aplicativo pai), o instalador do navegador Y acessará a rede e fará o download os arquivos necessários. Após a instalação, o navegador Y não terá nenhuma conexão de rede de acordo com as configurações do Firewall. Para proibir a atividade de rede do instalador do navegador Y como um processo filho, você deve adicionar uma regra de rede para o instalador do navegador Y.

Sobre o status de conexão de rede

O Firewall controla todas as conexões de rede do computador do usuário e atribui automaticamente um status a cada conexão de rede detectada.

A conexão de rede pode ter um dos seguintes tipos de status:

- **Rede pública**. Este status se aplica a redes que não são protegidas por nenhum aplicativo antivírus, firewalls ou filtros (por exemplo, redes de cyber cafés). Quando o usuário utiliza um computador que está conectado a uma rede desse tipo, o Firewall bloqueia o acesso a arquivos e impressoras desse computador. Os usuários externos também não conseguem acessar dados através de pastas compartilhadas e de acesso remoto à área de trabalho desse computador. O Firewall filtra a atividade de rede de cada aplicativo, de acordo com as regras de rede definidas para cada uma.

  Por padrão, o Firewall atribui o status *Rede pública* à Internet. Não é possível alterar o status da Internet.

- **Rede local**. Este status é atribuído às redes cujos usuários possuem confiança para acessar arquivos e impressoras nesse computador (por exemplo, uma rede LAN ou doméstica).

- **Rede confiável**. Este status se destina a uma rede segura, em que o computador não está exposto a ataques ou tentativas não autorizadas de acesso a dados. O Firewall permite qualquer atividade de rede dentro de redes com este status.

Alterar o status de conexão de rede

Para alterar o status da conexão de rede:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Firewall**.

   Na parte direita da janela, as configurações do componente Firewall são exibidas.
3. Clique no botão **Redes disponíveis**.

   A janela **Firewall** é exibida.
4. Selecione a conexão de rede cujo status deseja alterar.
5. No menu de contexto, selecione o status de conexão de rede:
   - **Rede pública**.
   - **Rede local**.
   - **Rede confiável**.
6. Na janela **Firewall**, clique em **OK**.

7. Para salvar as alterações, clique no botão **Salvar**.

Gerenciar regras de pacotes de rede

É possível efetuar as seguintes ações na gestão das regras de pacotes de rede:

- Criar uma nova regra de pacotes de rede.

  É possível criar uma nova regra de pacotes de rede criando um conjunto de condições e ações aplicadas a pacotes de rede e transmissões de dados.

- Ativar ou desativar uma regra de pacotes de rede.

  Todas as regras de pacotes de rede criadas pelo Firewall possuem o status *Ativada* por padrão. Quando uma regra de pacotes de rede é ativada, o Firewall aplica essa regra.

  É possível desativar qualquer regra de pacotes de rede marcada na lista de regras de pacotes de rede. Quando uma regra de pacotes de rede está desativada, o Firewall não aplica essa regra temporariamente.

  > É adicionada uma nova regra de pacotes de rede personalizada à lista de regras de pacotes de rede com o status *Ativada* por padrão.

- Editar as configurações de uma regra de pacotes de rede existente.

  Após a criação de uma regra de pacotes de rede, é sempre possível editar estas configurações e alterá-las, conforme necessário.

- Alterar a ação do Firewall para uma regra de pacotes de rede.

  Na lista de regras de pacotes de rede, é possível editar a ação efetuada pelo Firewall após detectar atividade de rede correspondente a uma regra de pacotes de rede específica.

- Alterar a prioridade de uma regra de pacotes de rede.

  É possível aumentar ou reduzir a prioridade de uma regra de pacotes de rede marcada na lista.

- Excluir uma regra de pacotes de rede.

  É possível excluir uma regra de pacotes de rede para impedir que o Firewall a aplique ao detectar atividade de rede e para impedir que esta regra seja exibida na lista de regras de pacotes de rede com o status *Desativada*.

Criar e editar uma regra de pacotes de rede

> Ao criar regras de pacotes de rede, lembre-se de que elas têm prioridade sobre as regras de rede para aplicativos.

Para criar ou editar uma regra de pacotes de rede:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione **Firewall**.

3. Clique no botão **Regras de pacotes de rede**.

4. A janela **Firewall** é aberta na guia **Regras de pacotes de rede**.

   Esta guia exibe uma lista de regras de pacotes de rede especificadas pelo Firewall.

5. Execute uma das seguintes ações:

   - Para criar uma nova regra de pacotes de rede, clique no botão **Adicionar**.
   - Para editar uma regra de pacotes de rede, selecione-a na lista de regras de rede e clique no botão **Editar**.

   A janela **Regra de rede** é exibida.

6. Na lista suspensa **Ação**, selecione a ação a ser executada pelo Firewall ao detectar este tipo de atividade de rede:

   - **Permitir**
   - **Bloquear**
   - **Por regras de aplicativos**.

7. No campo **Nome**, especifique o nome do serviço de rede da seguinte forma:

   - Clique no ícone , à direita do campo **Nome**, e selecione o nome do serviço de rede na lista suspensa.

     A lista suspensa inclui os serviços de rede que definem as conexões de rede mais utilizadas.

   - Insira manualmente o nome do serviço de rede no campo **Nome**.

8. Especifique o protocolo de transferência de dados:

   a. Marque a caixa de seleção **Protocolo**.

   b. Na lista suspensa, selecione o tipo de protocolo cuja atividade da rede será monitorada.

      O Firewall controla as conexões de rede que usam os protocolos TCP, UDP, ICMP, ICMPv6, IGMP e GRE.

      Se selecionar um serviço de rede na lista suspensa **Nome**, a caixa de seleção **Protocolo** será marcada automaticamente e a lista suspensa próxima à caixa de seleção será preenchida com um tipo de protocolo correspondente ao serviço de rede selecionado. Por padrão, a caixa de seleção **Protocolo** está desmarcada.

9. Na lista suspensa **Direção**, selecione a direção da atividade de rede monitorada.

   O Firewall controla as conexões de rede que usam as seguintes direções:

   - **Entrada (pacote)**.
   - **De entrada**.
   - **De entrada / De saída**
   - **Saída (pacote)**.
   - **De saída**.

10. Ao selecionar os protocolos do tipo ICMP ou ICMPv6, especifique o tipo e o código do pacote ICMP:

a. Marque a caixa de seleção **tipo ICMP** e selecione o tipo de pacote ICMP na lista suspensa.

b. Marque a caixa de seleção **código ICMP** e selecione o código do pacote ICMP na lista suspensa.

11. Ao selecionar os protocolos TCP ou UDP, especifique as portas dos computadores local e remoto entre os quais ocorrerá o monitoramento da conexão:

    a. Insira as porta do computador remoto no campo **Portas remotas**.

    b. Insira as paras do computador local no campo **Portas locais**.

12. Na tabela **Adaptadores de rede**, especifique as configurações dos adaptadores de rede a partir dos quais os pacotes de rede podem ser enviados ou que podem recebê-los. Para fazer isso, utilize os botões **Adicionar**, **Editar** e **Excluir**.

13. Se desejar restringir o controle de pacotes de rede com base no seu tempo de vida (TTL), marque a caixa de seleção **TTL** e, no campo ao lado dela, especifique o intervalo de valores do tempo de vida dos pacotes de rede de entrada e/ou de saída.

    Uma regra de rede controlará a transmissão dos pacotes de rede cujo tempo de vida não excede o valor especificado.

    Caso contrário, desmarque a caixa de seleção **TTL**.

14. Especifique os endereços de rede dos computadores remotos que podem enviar ou receber pacotes de rede. Para fazer isso, selecione um dos seguintes valores na lista suspensa **Endereços remotos**:

    - **Qualquer endereço**. A regra de rede controla os pacotes de rede enviados e/ou recebidos pelos computadores remotos com qualquer endereço IP.
    - **Endereços de sub-rede**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores remotos com endereços IP associados ao tipo de rede selecionado: **Redes confiáveis**, **Redes locais** ou **Redes públicas**.
    - **Endereços da lista**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores remotos com endereços IP que podem ser especificados na lista abaixo usando os botões **Adicionar**, **Editar** e **Excluir**.

15. Especifique os endereços de rede dos computadores com o Kaspersky Endpoint Security instalado, e que podem enviar e/ou receber pacotes de rede. Para fazer isso, selecione um dos seguintes valores na lista suspensa, **Endereços locais**:

    - **Qualquer endereço**. A regra de rede controla os pacotes de rede enviados e/ou recebidos por computadores com o Kaspersky Endpoint Security instalado e com qualquer endereço IP.
    - **Endereços da lista**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores que possuem o Kaspersky Endpoint Security instalado e com endereços IP que podem ser especificados na lista abaixo utilizando os botões **Adicionar**, **Editar** e **Excluir**.

    Às vezes um endereço local não pode ser obtido para aplicativos que trabalham com pacotes de rede. Se este for o caso, o valor da configuração **Endereços locais** será ignorado.

16. Se desejar que as ações da regra de rede sejam refletidas no relatório, marque a caixa de seleção **Registrar eventos**.

17. Na janela **Regra de rede**, clique em **OK**.

Ao criar uma nova regra de rede, a regra é exibida na guia **Regras de pacotes de rede** da janela **Firewall**. Por padrão, a nova regra de rede é colocada no final da lista de regras de pacotes de rede.

18. Na janela **Firewall**, clique em **OK**.

19. Para salvar as alterações, clique no botão **Salvar**.

Ativar ou desativar uma regra de pacotes de rede

Para ativar ou desativar uma regra de pacotes de rede:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Firewall**.
   Na parte direita da janela, as configurações do componente Firewall são exibidas.

3. Clique no botão **Regras de pacotes de rede**.
   A janela **Firewall** é aberta na guia **Regras de pacotes de rede**.

4. Selecione a regra de pacotes de rede necessária na lista.

5. Execute uma das seguintes ações:

   - Para ativar a rede, selecione a caixa de seleção ao lado do nome da regra de pacotes de rede.
   - Para desativar a rede, remova a seleção da caixa de seleção ao lado do nome da regra de pacotes de rede.

6. Clique em **OK**.

7. Para salvar as alterações, clique no botão **Salvar**.

Alterar a ação do Firewall para uma regra de pacotes de rede

Para alterar a ação do Firewall aplicada a uma regra de pacotes de rede:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Firewall**.
   Na parte direita da janela, as configurações do componente Firewall são exibidas.

3. Clique no botão **Regras de pacotes de rede**.
   A janela **Firewall** é aberta na guia **Regras de pacotes de rede**.

4. Na lista, selecione a regra do pacote de rede cuja ação você deseja alterar.

5. Na coluna **Permissão**, clique com o botão direito do mouse para exibir o menu de contexto e selecione a ação que você pretende atribuir:

   - **Permitir**

- **Bloquear**
- **De acordo com a regra de aplicativos**
- **Registrar eventos**

6. Na janela **Firewall**, clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Alterar a prioridade de uma regra de pacotes de rede

A prioridade de uma regra de pacotes de rede é determinada pela sua posição na lista de regras de pacotes de rede. A regra de rede no topo da lista de regras de rede tem prioridade em relação às demais.

Todas as regras de pacotes de rede criadas manualmente são adicionadas ao fim da lista de regras de pacotes de rede, sendo estas precedidas pelas demais.

O Firewall executa as regras na ordem em que aparecem na lista de regras de pacotes de rede, ou seja, de cima para baixo. De acordo com cada regra de rede processada aplicada a uma conexão de rede específica, o Firewall permite ou bloqueia o acesso à rede ao endereço e à porta que estão indicados nas configurações desta conexão de rede.

Para alterar a prioridade das regras de pacotes de rede:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Firewall**.

   Na parte direita da janela, as configurações do componente Firewall são exibidas.
3. Clique no botão **Regras de pacotes de rede**.

   A janela **Firewall** é aberta na guia **Regras de pacotes de rede**.
4. Na lista, selecione a regra do pacote de rede cuja prioridade você deseja alterar.
5. Use os botões **Mover para cima** e **Mover para baixo** para mover a regra de rede de um aplicativo para o local desejado na lista de regras de rede de aplicativos.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Gerenciar as regras de rede de aplicativos

Por padrão, o Kaspersky Endpoint Security reúne todos os aplicativos instalados no computador do usuário pelo nome do fornecedor do aplicativo cujo arquivo ou atividade de rede é monitorado. Os grupos de aplicativos são, por sua vez, categorizados em grupos confiáveis. Todos os aplicativos e grupos de aplicativos herdam as propriedades do seu grupo pai: regras de controle de aplicativos, regras de rede para aplicativos e prioridade de execução.

Por padrão, o componente Firewall aplica as regras de rede de grupo quando filtra a atividade de rede de todos os aplicativos dentro do grupo, de forma similar ao componente Controle de Privilégios de Aplicativo. As regras de rede de grupo de aplicativos definem os direitos de aplicativos dentro do grupo para acessar diferentes conexões de rede.

Por padrão, o Firewall cria um conjunto de regras de rede para cada grupo de aplicativos detectado pelo Kaspersky Endpoint Security no computador. É possível alterar a ação do Firewall aplicada às regras de rede de grupo de aplicativos criadas por padrão. Não é possível editar, remover, desativar ou alterar a prioridade das regras de rede de grupo de aplicativos criadas por padrão.

Você também pode criar uma regra de rede para um aplicativo individual. Tal regra terá uma prioridade mais alta do que a regra de rede do grupo ao qual o aplicativo pertence.

É possível efetuar as seguintes ações enquanto gerencia as regras de rede dos aplicativos:

- Criar uma nova regra de rede.

  Você pode criar uma nova regra de rede pela qual o Firewall deve regular a atividade da rede do aplicativo ou aplicativos que pertencem ao grupo selecionado de aplicativos.

- Ativar ou desativar uma regra de rede.

  Todas as regras de rede são adicionadas à lista de regras de rede dos aplicativos com status *Ativado*. Quando uma regra de rede é ativada, o Firewall aplica essa regra.

  Você pode desativar uma regra de rede que foi criada manualmente. Quando uma regra de rede está desativada, o Firewall não aplica esta regra temporariamente.

- Alterar as configurações de uma regra de rede.

  Após a criação de uma nova regra de rede, é sempre possível retornar às configurações e modificá-las conforme necessário.

- Alterar a ação do Firewall para uma regra de rede.

  Na lista de regras de rede, é possível editar a ação aplicada pelo Firewall à regra de rede mediante a detecção de atividade de rede nesse aplicativo ou grupo de aplicativos.

- Alterar a prioridade de uma regra de rede.

  É possível aumentar ou abaixar a prioridade de uma regra de rede personalizada.

- Excluir uma regra de rede.

  É possível excluir uma regra de rede personalizada para impedir que o Firewall aplique essa regra de rede ao aplicativo selecionado ou ao grupo de aplicativos, mediante detecção de atividade de rede, e para impedir que essa regra seja exibida na lista de regras de rede de aplicativos.

Criar e editar uma regra de rede de um aplicativo

Para criar ou editar uma regra de rede em um grupo de aplicativos:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Firewall**.

3. Clique no botão **Regras de rede de aplicativos**.

   A janela **Firewall** é aberta na guia **Regras de Controle de Aplicativos**.

4. Na lista de aplicativos, selecione o aplicativo ou grupo de aplicativos em que deseja criar ou editar de uma regra de rede.

5. Clique com o botão direito para exibir o menu de contexto e selecione **Regras de Aplicativo** ou **Regras de grupos** dependendo do que você tem de fazer.

   Isto abre as **Regras de Controle de Aplicativos** ou a janela **Regras de controle de grupo de aplicativos**.

6. Na janela que é aberta, selecione a guia **Regras de rede**.

7. Execute uma das seguintes ações:

   - Para criar uma nova regra de rede, clique no botão **Adicionar**.
   - Para editar uma regra de rede, selecione-a na lista de regras de rede e clique no botão **Editar**.

   A janela **Regra de rede** é exibida.

8. Na lista suspensa **Ação**, selecione a ação a ser executada pelo Firewall ao detectar este tipo de atividade de rede:

   - **Permitir**
   - **Bloquear**

9. No campo **Nome**, especifique o nome do serviço de rede da seguinte forma:

   - Clique no ícone , à direita do campo **Nome**, e selecione o nome do serviço de rede na lista suspensa.

     A lista suspensa inclui os serviços de rede que definem as conexões de rede mais utilizadas.

   - Insira manualmente o nome do serviço de rede no campo **Nome**.

10. Especifique o protocolo de transferência de dados:

    a. Marque a caixa de seleção **Protocolo**.

    b. Na lista suspensa, selecione o tipo de protocolo em que a atividade da rede será monitorada.

       O Firewall controla as conexões de rede que usam os protocolos TCP, UDP, ICMP, ICMPv6, IGMP e GRE.

       Se selecionar um serviço de rede na lista suspensa **Nome**, a caixa de seleção **Protocolo** será marcada automaticamente e a lista suspensa próxima à caixa de seleção será preenchida com um tipo de protocolo correspondente ao serviço de rede selecionado. Por padrão, a caixa de seleção **Protocolo** está desmarcada.

11. Na lista suspensa **Direção**, selecione a direção da atividade de rede monitorada.

    O Firewall controla as conexões de rede que usam as seguintes direções:

    - **De entrada**.
    - **De entrada / De saída**.
    - **De saída**.

12. Ao selecionar os protocolos do tipo ICMP ou ICMPv6, especifique o tipo e o código do pacote ICMP:

a. Marque a caixa de seleção **tipo ICMP** e selecione o tipo de pacote ICMP na lista suspensa.

b. Marque a caixa de seleção **código ICMP** e selecione o código do pacote ICMP na lista suspensa.

13. Ao selecionar os protocolos TCP ou UDP, especifique as portas dos computadores local e remoto entre os quais ocorrerá o monitoramento da conexão:

    a. Insira as porta do computador remoto no campo **Portas remotas**.

    b. Insira as paras do computador local no campo **Portas locais**.

14. Especifique os endereços de rede dos computadores remotos que podem enviar ou receber pacotes de rede. Para fazer isso, selecione um dos seguintes valores na lista suspensa **Endereços remotos**:

    - **Qualquer endereço**. A regra de rede controla os pacotes de rede enviados e/ou recebidos pelos computadores remotos com qualquer endereço IP.
    - **Endereços de sub-rede**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores remotos com endereços IP associados ao tipo de rede selecionado: **Redes confiáveis**, **Redes locais** ou **Redes públicas**.
    - **Endereços da lista**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores remotos com endereços IP que podem ser especificados na lista abaixo usando os botões **Adicionar**, **Editar** e **Excluir**.

15. Especifique os endereços de rede dos computadores com o Kaspersky Endpoint Security instalado, e que podem enviar e/ou receber pacotes de rede. Para fazer isso, selecione um dos seguintes valores na lista suspensa, **Endereços locais**:

    - **Qualquer endereço**. A regra de rede controla os pacotes de rede enviados e/ou recebidos por computadores com o Kaspersky Endpoint Security instalado e com qualquer endereço IP.
    - **Endereços da lista**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores que possuem o Kaspersky Endpoint Security instalado e com endereços IP que podem ser especificados na lista abaixo utilizando os botões **Adicionar**, **Editar** e **Excluir**.

    Às vezes um endereço local não pode ser obtido para aplicativos que trabalham com pacotes de rede. Se este for o caso, o valor da configuração **Endereços locais** será ignorado.

16. Se desejar que as ações da regra de rede sejam refletidas no relatório, marque a caixa de seleção **Registrar eventos**.

17. Na janela **Regra de rede**, clique em **OK**.

    Se você criou uma nova regra de rede, a regra é exibida na guia **Regras de rede**.

18. Clique em **OK** na janela **Regras de controle de grupo de aplicativos**, se a regra for destinada a um grupo de aplicativos, ou na janela **Regras de controle de aplicativos**, se a regra for destinada a um aplicativo.

19. Na janela **Firewall**, clique em **OK**.

20. Para salvar as alterações, clique no botão **Salvar**.

Ativar e desativar uma regra de rede de aplicativo

Para ativar ou desativar uma regra de rede de um aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Firewall**.

   Na parte direita da janela, as configurações do componente Firewall são exibidas.
3. Clique no botão **Regras de rede de aplicativos**.

   A janela **Firewall** é aberta na guia **Regras de Controle de Aplicativos**.
4. Na lista, selecione o aplicativo ou grupo de aplicativos em que deseja ativar ou desativar uma regra de rede.
5. Clique com o botão direito para exibir o menu de contexto e selecione **Regras de Aplicativo** ou **Regras de grupos** dependendo do que você tem de fazer.

   Isto abre as **Regras de Controle de Aplicativos** ou a janela **Regras de controle de grupo de aplicativos**.
6. Na janela que é aberta, selecione a guia **Regras de rede**.
7. Na lista de regras de rede para grupos de aplicativos, selecione a regra de rede relevante.
8. Execute uma das seguintes ações:
   - Se desejar ativar a regra, marque a caixa de seleção junto ao nome da regra de rede.
   - Se desejar desativar a regra, desmarque a caixa de seleção junto do nome da regra de rede.

     Não é possível desativar uma regra de rede de grupo de aplicativos criada pelo Firewall por padrão.
9. Clique em **OK** na janela **Regras de controle de grupo de aplicativos**, se a regra for destinada a um grupo de aplicativos, ou na janela **Regras de controle de aplicativos**, se a regra for destinada a um aplicativo.
10. Na janela **Firewall**, clique em **OK**.
11. Para salvar as alterações, clique no botão **Salvar**.

Alterar a ação do Firewall para uma regra de rede de um aplicativo

É possível alterar a ação do Firewall que é aplicada a todas as regras de rede para um aplicativo ou grupo de aplicativos que foi criado por padrão; e alterar a ação do Firewall para uma única regra de rede personalizada para um aplicativo ou grupo de aplicativos.

Para modificar a ação de Firewall de todas as regras de rede de um aplicativo ou o grupo de aplicativos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Firewall**.

Na parte direita da janela, as configurações do componente Firewall são exibidas.

3. Clique no botão **Regras de rede de aplicativos**.

   A janela **Firewall** é aberta na guia **Regras de Controle de Aplicativos**.

4. Se desejar modificar a ação do Firewall que é aplicada a todas as regras de rede que são criadas por padrão, selecione um aplicativo ou grupo de aplicativos na lista. As regras de rede criadas manualmente não são alteradas.

5. Na coluna **Rede**, clique para exibir o menu de contexto e selecione a ação que você pretende atribuir:

   - **Herdar**
   - **Permitir**
   - **Bloquear**

6. Clique em **OK**.

7. Para salvar as alterações, clique no botão **Salvar**.

Para modificar a resposta do Firewall a uma regra de rede de um aplicativo ou grupo de aplicativos:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione **Firewall**.

   Na parte direita da janela, as configurações do componente Firewall são exibidas.

3. Clique no botão **Regras de rede de aplicativos**.

   A janela **Firewall** é aberta na guia **Regras de Controle de Aplicativos**.

4. Na lista, selecione o aplicativo ou o grupo de aplicativos para os quais você deseja modificar a ação de uma regra de rede.

5. Clique com o botão direito para exibir o menu de contexto e selecione **Regras de Aplicativo** ou **Regras de grupos** dependendo do que você tem de fazer.

   Isto abre as **Regras de Controle de Aplicativos** ou a janela **Regras de controle de grupo de aplicativos**.

6. Na janela que é aberta, selecione a guia **Regras de rede**.

7. Selecione a regra de rede para a qual você deseja modificar a ação do Firewall.

8. Na coluna **Permissão**, clique com o botão direito do mouse para exibir o menu de contexto e selecione a ação que você pretende atribuir:

   - **Permitir**
   - **Bloquear**
   - **Registrar eventos**

9. Clique em **OK** na janela **Regras de controle de grupo de aplicativos**, se a regra for destinada a um grupo de aplicativos, ou na janela **Regras de controle de aplicativos**, se a regra for destinada a um aplicativo.

10. Na janela **Firewall**, clique em **OK**.

11. Para salvar as alterações, clique no botão **Salvar**.

Alterar a prioridade de uma regra de rede de um aplicativo

A prioridade de uma regra de rede é determinada pela sua posição na lista de regras de rede. O Firewall executa as regras na ordem em que aparecem na lista de regras de rede, de cima para baixo. De acordo com cada regra de rede processada aplicada a uma conexão de rede específica, o Firewall ou permite ou bloqueia o acesso ao endereço e à porta que estão indicados nas configurações desta conexão de rede.

As regras de rede criadas manualmente têm uma prioridade mais alta do que regras de rede padrão.

Não é possível alterar a prioridade das regras de rede de grupo de aplicativos criadas por padrão.

Para alterar a prioridade de uma regra de rede:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Firewall**.

   Na parte direita da janela, as configurações do componente Firewall são exibidas.
3. Clique no botão **Regras de rede de aplicativos**.

   A janela **Firewall** é aberta na guia **Regras de Controle de Aplicativos**.
4. Na lista de aplicativos, selecione o aplicativo ou grupo de aplicativos em que deseja alterar a prioridade de uma regra de rede.
5. Clique com o botão direito para exibir o menu de contexto e selecione **Regras de Aplicativo** ou **Regras de grupos** dependendo do que você tem de fazer.

   Isto abre as **Regras de Controle de Aplicativos** ou a janela **Regras de controle de grupo de aplicativos**.
6. Na janela que é aberta, selecione a guia **Regras de rede**.
7. Selecione a regra de rede cuja prioridade deseja alterar.
8. Use os botões **Mover para cima** e **Mover para baixo** para mover a regra de rede para o local pretendido na lista de regras de rede.
9. Clique em **OK** na janela **Regras de controle de grupo de aplicativos**, se a regra for destinada a um grupo de aplicativos, ou na janela **Regras de controle de aplicativos**, se a regra for destinada a um aplicativo.
10. Na janela **Firewall**, clique em **OK**.
11. Para salvar as alterações, clique no botão **Salvar**.

Monitor de Rede

Esta seção contém informações sobre o Monitor de Rede e as instruções para definir as configurações do componente.

Sobre o Monitor de Rede

O *Monitor de Rede* é uma ferramenta desenvolvida para exibir informações sobre a atividade do computador de um usuário em tempo real.

Executar o Monitor de Rede

Para iniciar o Monitor de Rede:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Proteção**.

   A seção **Proteção** é exibida.
4. Clique com o botão direito na linha **Firewall** para abrir o menu de contexto de operações do Firewall.
5. No menu de contexto, selecione **Monitor de Rede**.

   A janela **Monitor de Rede** abre. Nesta janela, as informações sobre a atividade de rede são exibidas em quatro guias:

   - A guia **Atividade de rede** exibe todas as conexões de rede atuais estabelecidas com o computador. São exibidos o tráfego de entrada e de saída das conexões de rede.
   - A guia **Portas abertas** lista todas as portas de rede abertas do computador.
   - A guia **Tráfego de rede** exibe o volume do tráfego de entrada e de saída entre o computador do usuário e outros computadores da rede nos quais o usuário está conectado atualmente.
   - A guia **Computadores bloqueados** lista os endereços IP de computadores remotos cuja atividade de rede foi interrompida pelo Bloqueio de Ataque de Rede ao detectar uma tentativa de ataque de rede destes endereços IP.

Bloqueio de Ataque de Rede

Esta seção contém informações sobre o Bloqueio de Ataque de Rede e as instruções para definir as configurações do componente.

Sobre o Bloqueio de Ataque de Rede

O Bloqueio de Ataque de Rede verifica no tráfego de entrada atividades típicas de ataques de rede. Ao detectar uma tentativa de ataque de rede ao computador, o Kaspersky Endpoint Security bloqueia a atividade de rede do computador em ataque. A sua tela então exibe um aviso que afirma que um ataque de rede foi tentado, e mostra informações sobre o computador em ataque.

O tráfego de rede do computador de ataque é bloqueado por uma hora. Para editar as configurações de bloqueio de um computador em ataque:

As descrições dos tipos de ataques de rede atuais e formas de combatê-los estão disponibilizadas nos bancos de dados do Kaspersky Endpoint Security. A lista de ataques de rede que o componente Bloqueio de Ataque de Rede detecta é atualizada durante atualizações de módulo do aplicativo e do banco de dados.

Ativar e desativar o Bloqueio de Ataque de Rede

Por padrão, o Bloqueio de Ataque de Rede está ativado e funciona no modo normal. Se necessário, é possível desativar o Bloqueio de Ataque de Rede.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

Para ativar ou desativar o Bloqueio de Ataque de Rede, execute o seguinte na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Proteção**.

   A seção **Proteção** é exibida.
4. Clique com o botão direito do mouse na linha do **Bloqueio de Ataque de Rede** para exibir o menu de contexto das ações do Bloqueio de Ataque de Rede.
5. Execute uma das seguintes ações:

   - Para ativar o Bloqueio de Ataque de Rede, selecione **Iniciar** no menu de contexto.

     O ícone de status do componente , exibido à esquerda na linha do **Bloqueio de Ataque de Rede**, muda para o ícone .
   - Para desativar o Bloqueio de Ataque de Rede, selecione **Interromper** no menu de contexto.

O ícone de status do componente , exibido à esquerda na linha do **Bloqueio de Ataque de Rede**, muda para o ícone .

Para ativar ou desativar o Bloqueio de Ataque de Rede na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Bloqueio de Ataque de Rede**.

   As configurações do Bloqueio de Ataque de Rede são exibidas na parte direita da janela.
3. Faça o seguinte:
   - Para ativar o Bloqueio de Ataque de Rede, marque a caixa de seleção **Ativar o Bloqueio de Ataque de Rede**.
   - Para desativar o Bloqueio de Ataque de Rede, desmarque a caixa de seleção **Ativar o Bloqueio de Ataque de Rede**.
4. Para salvar as alterações, clique no botão **Salvar**.

Configurações do Bloqueio de ataque de rede

Você pode executar as seguintes ações para definir as configurações do Bloqueio de Ataque de Rede:

- Editar as configurações usadas no bloqueio de um computador atacante.
- Gerar uma lista de endereços de exclusões do bloqueio.

Editar as configurações usadas no bloqueio de um computador atacante

Para editar as configurações de bloqueio de um computador de ataque:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Bloqueio de Ataque de Rede**.

   As configurações do Bloqueio de Ataque de Rede são exibidas na parte direita da janela.
3. Marque a caixa de seleção **Adicionar o computador de ataque à lista de computadores bloqueados por**.

   Se esta caixa de seleção está marcada, ao detectar uma tentativa de ataque de rede, o Bloqueio de Ataque de Rede impede o tráfego de rede originado do computador de ataque durante o período de tempo de bloqueio especificado. Esta ação protege o computador automaticamente contra a ocorrência de ataques de rede futuros que se originem do mesmo endereço.

   Se esta caixa de seleção está desmarcada, ao detectar uma tentativa de ataque de rede, o Bloqueio de Ataque de Rede não ativa a proteção automaticamente contra a ocorrência de ataques de rede futuros que se originem do mesmo endereço.
4. Você pode alterar o período de tempo do bloqueio do computador de ataque no campo próximo à caixa de seleção **Adicionar o computador de ataque à lista de computadores bloqueados por**.
5. Para salvar as alterações, clique no botão **Salvar**.

Configurar endereços de exclusões de bloqueio

Para configurar endereços de exclusão do bloqueio:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Bloqueio de Ataque de Rede**.

   As configurações do Bloqueio de Ataque de Rede são exibidas na parte direita da janela.
3. Clique no botão **Exclusões**.

   A janela **Exclusões** é exibida.
4. Execute uma das seguintes ações:

   - Se desejar adicionar um novo endereço IP, clique no botão **Adicionar**.
   - Se desejar editar um endereço IP adicionado anteriormente, selecione-o na lista de endereços e clique no botão **Editar**.

   A janela **Endereço IP** é exibida.
5. Insira o endereço IP do computador a partir do qual os ataques de rede não devem ser bloqueados.
6. Na janela **Endereço IP**, clique em **OK**.
7. Na janela **Exclusões**, clique em **OK**.
8. Para salvar as alterações, clique no botão **Salvar**.

Prevenção contra ataque BadUSB

Esta seção contém informações sobre o componente Prevenção contra ataque BadUSB.

Sobre a Prevenção contra ataque BadUSB

Alguns vírus modificam o firmware dos dispositivos USB para enganar o sistema operacional em detectar o dispositivo USB como um teclado.

O componente Prevenção contra ataque BadUSB previne dispositivos de USB infectados que emulam um teclado de unir-se ao computador.

Quando um dispositivo USB é conectado ao computador e identificado pelo aplicativo como um teclado, o aplicativo solicita que o usuário insira um código numérico gerado pelo aplicativo nesse teclado ou usando um teclado virtual (caso esteja disponível). Esse procedimento é conhecido como autorização do teclado. O aplicativo permite a utilização de um teclado autorizado e bloqueia um teclado que não tenha sido autorizado.

A Prevenção contra ataque BadUSB é executada em modo de segundo plano assim que esse componente é instalado. Se o aplicativo não for sujeito a uma política do Kaspersky Security Center, você pode ativar ou desativar a Prevenção contra ataque BadUSB fazendo uma pausa temporária e retomando a proteção do computador e o controle.

Instalar o componente Prevenção contra ataque BadUSB

Se você tiver selecionado instalação básica ou padrão durante a instalação do Kaspersky Endpoint Security, o componente Prevenção contra ataque BadUSB não estará disponível. Para instalá-lo, você deve modificar o conjunto de componentes do aplicativo.

Para instalar o componente Prevenção contra ataque BadUSB:

1. No menu **Iniciar**, selecione Aplicativos → Kaspersky Endpoint Security 10 for Windows → **Modificar, Reparar ou Remover**.

   O Assistente de Instalação inicia.

2. Na janela **Modificar, Reparar ou Remover o aplicativo** do Assistente de Instalação do Aplicativo, clique no botão **Modificar**.

   É exibida a janela **Instalação personalizada** do Assistente de Instalação do Aplicativo.

3. No menu de contexto do ícone próximo do nome do componente **Prevenção contra ataque BadUSB**, selecione a opção **O recurso será instalado no disco rígido local**.

4. Clique no botão **Avançar**.

5. Siga as instruções do Assistente de Instalação.

Ativar e desativar Prevenção contra ataque BadUSB

Para ativar ou desativar a Proteção contra ataque BadUSB:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Prevenção contra ataque BadUSB**.

   As configurações de Prevenção contra ataque BadUSB são exibidas na parte direita da janela.
3. Execute uma das seguintes ações:

   - Para ativar a Prevenção contra ataque BadUSB, marque a caixa de seleção **Ativar prevenção contra ataque BadUSB**.
   - Para desativar a Prevenção contra ataque BadUSB, desmarque a caixa de seleção **Ativar prevenção contra ataque BadUSB**.
4. Para salvar as alterações, clique no botão **Salvar**.

Permitir e proibir a utilização do Teclado Virtual na autorização

O Teclado Virtual deveria apenas ser utilizado para autorização de dispositivos USB que não suportam a entrada de caracteres aleatórios (por exemplo, leitores de códigos de barras). Não é recomendado utilizar o Teclado Virtual para autorização de dispositivos USB desconhecidos.

Para permitir ou proibir a utilização do Teclado Virtual na autorização:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Proteção antivírus**, selecione a subseção **Prevenção contra ataque BadUSB**.

   As configurações do componente são exibidas na parte direita da janela.
3. Execute uma das seguintes ações:

   - Marque a caixa de seleção **Proibido usar o Teclado em Tela para autorização** para bloquear a utilização do Teclado Virtual para autorização.
   - Desmarque a caixa de seleção **Proibido usar o Teclado em Tela para autorização** para permitir a utilização do Teclado Virtual para autorização.
4. Para salvar as alterações, clique no botão **Salvar**.

Autorização do teclado

Os dispositivos USB identificados pelo sistema operacional como teclados e conectados ao computador antes da instalação do componente Prevenção contra ataque BadUSB são considerados autorizados após instalação do componente.

O aplicativo requer autorização do dispositivo USB conectado que foi identificado pelo sistema operacional como um teclado apenas se a solicitação de autorização do teclado USB estiver ativada. O usuário não pode utilizar um teclado não autorizado até que ele esteja autorizado.

Se a solicitação de autorização do teclado USB estiver desativada, o usuário poderá utilizar todos os teclados conectados. Imediatamente após a solicitação de autorização do teclado USB estar ativada, o aplicativo exibirá uma solicitação de autorização de cada teclado não autorizado que estiver conectado.

Para autorizar um teclado:

1. Com a autorização do teclado USB ativada, conecte o teclado a uma porta USB.

   A janela **Autorização do teclado <nome do teclado>** é aberta com os detalhes do teclado conectado e um código numérico para a sua autorização.

2. Insira o código numérico gerado aleatoriamente na janela de autorização a partir do teclado conectado ou do Teclado Virtual (se disponível).

3. Clique em **OK**.

   Se o código tiver sido inserido corretamente, o aplicativo salvará os parâmetros de identificação – VID/PID do teclado e o número da porta à qual ele foi conectado – na lista de teclados autorizados. A autorização não precisa ser repetida quando o teclado é reconectado ou após o sistema operacional ser reiniciado.

   > Quando o teclado autorizado é conectado à uma porta USB diferente do computador, o aplicativo exibe uma solicitação para autorização desse teclado novamente.

   Se o código numérico tiver sido inserido de forma incorreta, o aplicativo gerará um novo código. Estão disponíveis três tentativas para inserir o código numérico. Se o código numérico for inserido de forma incorreta três vezes seguidas ou se a janela **Autorização do teclado <nome do teclado>** for fechada, o aplicativo bloqueará a entrada desse teclado. Quando o teclado é reconectado ou quando o sistema operacional é reiniciado, o aplicativo solicitará ao usuário para realizar a autorização do teclado novamente.

Controle de Inicialização de Aplicativo

Esta seção contém informações sobre o Controle de Inicialização de Aplicativo e as instruções para definir as configurações do componente.

Sobre o Controle de Inicialização de Aplicativo

O componente Controle de Inicialização de Aplicativo monitora tentativas do usuário de iniciar aplicativos e regula a inicialização de aplicativos usando *Regras de Controle de Inicialização de Aplicativos*.

A inicialização de aplicativos cujas configurações não correspondem a nenhuma das regras do Controle de Inicialização de Aplicativos é gerenciada pelo modo operacional selecionado do componente. *O modo de Lista negra* é selecionado por padrão. Esse modo permite que todos usuários iniciem aplicativos.

Todas as tentativas de usuário de iniciarem aplicativos são registradas em relatórios.

Ativar e desativar o Controle de Inicialização de Aplicativo

Embora o Controle de Inicialização de Aplicativo esteja desativado por padrão, é possível ativá-lo, se necessário.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

Para ativar ou desativar o Controle de Inicialização de Aplicativo na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Controle de Endpoints**.

   A seção **Controle de Endpoints** é exibida.
4. Clique com o botão direito do mouse para abrir o menu de contexto da linha com as informações sobre o componente Controle de Inicialização de Aplicativo.

   Será aberto um menu para a seleção de ações.
5. Execute uma das seguintes ações:

   - Para ativar o Controle de Inicialização de Aplicativo, selecione **Iniciar** no menu.

     O ícone de status do componente , exibido à esquerda na linha do **Controle de Inicialização de Aplicativo**, muda para o ícone .
   - Para desativar o Controle de Inicialização de Aplicativo, selecione **Interromper** no menu.

     O ícone de status do componente , exibido à esquerda na linha do **Controle de Inicialização de Aplicativo**, muda para o ícone .

Para ativar ou desativar o Controle de Inicialização de Aplicativo na janela de configuração do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Inicialização de Aplicativo**.

   Na parte direita da janela, serão exibida as configurações do componente Controle de Inicialização de Aplicativo.
3. Execute uma das seguintes ações:

   - Para ativar o Controle de Inicialização de Aplicativo, marque a caixa de seleção **Ativar o Controle de Inicialização de Aplicativo**.
   - Para desativar o Controle de Inicialização de Aplicativo, desmarque a caixa de seleção **Ativar o Controle de Inicialização de Aplicativo**.
4. Para salvar as alterações, clique no botão **Salvar**.

Limitações de funcionalidade do Controle de Inicialização de Aplicativo

A operação do componente Controle de Inicialização de Aplicativo é limitada nos seguintes casos:

- Quando a versão do aplicativo é atualizada, a importação de configurações do componente Controle de Inicialização de Aplicativo não é suportada.

  Para restaurar a funcionalidade Controle de Inicialização de Aplicativo, você deve reconfigurar as configurações do componente.

- Se não houver conexão com os servidores KSN, o Kaspersky Endpoint Security recebe informações sobre a reputação dos aplicativos e os seus módulos somente dos bancos de dados locais. Se os bancos de dados locais não tiverem informações sobre o aplicativo, o aplicativo não será categorizado em um grupo confiável.

  A categorização de aplicativos quando há uma conexão com servidores KSN pode ser diferente da sua categorização quando não há conexão com KSN.

- No banco de dados de Kaspersky Security Center, informações de 150.000 arquivos processados podem ser armazenadas. Uma vez que este número de registros for alcançado, os novos arquivos não serão processados. Para retomar operações de inventário, você deve excluir os arquivos que foram anteriormente inventariados no banco de dados do Kaspersky Security Center do computador no qual o Kaspersky Endpoint Security está instalado.

- O componente não controla a inicialização de scripts a menos que o script seja enviado ao interpretador via a linha de comando.

  Se a inicialização de um interpretador for permitida por Regras de Controle de Inicialização de Aplicativos, o componente não bloqueará um script iniciado neste interpretador.

- O componente não controla os scripts de inicialização dos interpretadores que não são suportador por Kaspersky Endpoint Security.

  O Kaspersky Endpoint Security suporta os seguintes interpretadores:

  - Java
  - PowerShell

  Os seguintes tipos de interpretadores são suportados:

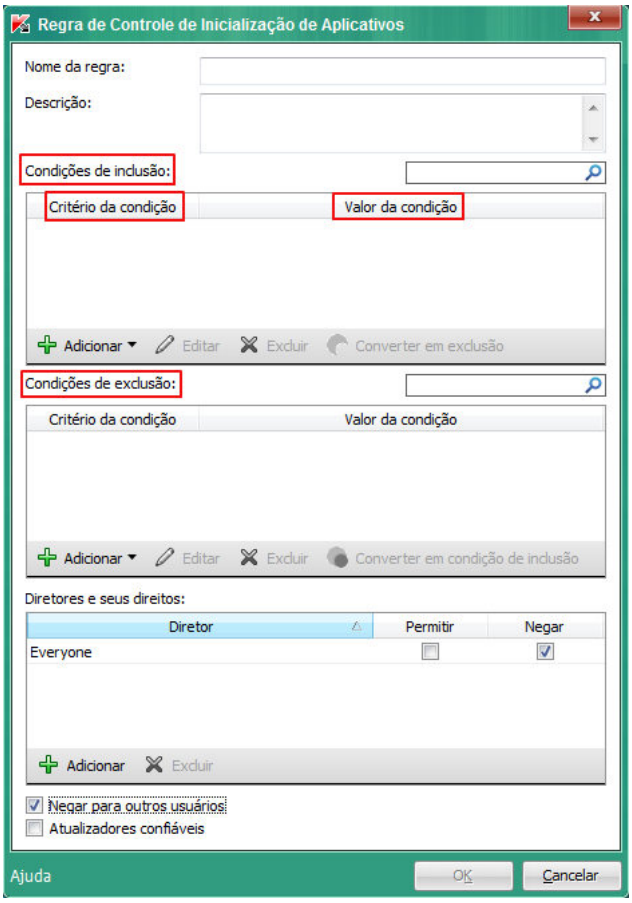
  - { cCmdLineParser::itCmd, _T("%ComSpec%") };
  - { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
  - { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
  - { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
  - { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
  - { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
  - { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
  - { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
  - { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
  - { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
  - { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
  - { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
  - { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
  - { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

Sobre as Regras de Controle de Inicialização de Aplicativos

O Kaspersky Endpoint Security controla a inicialização de aplicativos por usuários através de regras. Uma regra de Controle de Inicialização de Aplicativos especifica as condições de acionamento e a ação realizada pelo Controle de Inicialização de Aplicativo quando a regra é acionada (permitindo ou bloqueando a inicialização do aplicativo pelos usuários).

Condições de acionamento da regra

Uma condição para acionar a regra tem a seguinte correspondência: tipo de condição - critério de condição - valor de condição (veja a figura abaixo). Com base nas condições de acionamento de regra, o Kaspersky Endpoint Security aplica (ou não aplica) uma regra a um aplicativo.



Regra de Controle de Inicialização de Aplicativos. Parâmetros de condição de acionamento da regra

As regras usam as condições de inclusão e exclusão:

- *Condições de inclusão*. O Kaspersky Endpoint Security aplica a regra ao aplicativo se o aplicativo corresponder a pelo menos uma das condições de inclusão.

- *Condições de exclusão*. O Kaspersky Endpoint Security não aplica a regra ao aplicativo se o aplicativo corresponder a pelo menos uma das condições de exclusão e não corresponder a nenhuma das condições de inclusão.

Condições de acionamento da regra são criadas usando critérios. Os critérios a seguir são usados para criar regras no Kaspersky Endpoint Security:

- Caminho para a pasta que contém o arquivo executável do aplicativo ou caminho para o arquivo executável do aplicativo.
- Metadados: nome do arquivo executável do aplicativo, versão do arquivo executável do aplicativo, versão do aplicativo e fornecedor do aplicativo.
- Hash do arquivo executável de um aplicativo.
- Certificado: emissor, diretor, impressão digital.
- Inclusão do aplicativo na Categoria KL.
- Localização do arquivo executável do aplicativo em uma unidade removível.

O valor do critério deve ser especificado para cada critério usado na condição. Se os parâmetros do aplicativo a serem iniciados corresponderem aos valores dos critérios especificados em condições de inclusão, a regra será acionada. Nesse caso, o Controle de Inicialização de Aplicativo realiza a ação especificada na regra. Se os parâmetros de aplicativo coincidirem com os valores de critérios especificados na condição de exclusão, o Controle de Inicialização de Aplicativo não controlará a inicialização do aplicativo.

As decisões tomadas pelo componente Controle de Inicialização de Aplicativo quando uma regra é acionada

Quando uma regra é acionada, o Controle de Inicialização de Aplicativo permite que os usuários (ou grupos de usuários) iniciem aplicativos ou bloqueia a inicialização de acordo com a regra. Você pode selecionar usuários individuais ou grupos de usuários que podem ou não iniciar aplicativos que acionam uma regra.

Se uma regra que não especifica quais usuários têm permissão para iniciar aplicativos que satisfaçam à regra, ela é denominada regra de *bloqueio*.

A regra que não especifica nenhum usuário que não tem permissão para iniciar aplicativos que correspondem à regra, ela é chamada de regra de *permissão*.

A prioridade da regra de bloqueio é mais alta do que a de permissão. Por exemplo, se a regra de permissão do Controle de Inicialização de Aplicativo tiver sido especificada para um grupo de usuários, enquanto a regra de bloqueio do Controle de Inicialização de Aplicativo foi especificada para um usuário neste grupo de usuários, esse usuário será impedido de iniciar o aplicativo.

Status operacional de uma regra

As Regras de Controle de Inicialização de Aplicativos podem ter um dos dois valores de status seguintes:

- **Ativado.**

  Este status operacional significa que a regra está ativada.

- **Desativado.**

  Este status significa que a regra está desativada.

Regras de Controle de Inicialização de Aplicativos padrão

Por padrão, o Controle de Inicialização de Aplicativo funciona no modo Lista negra. Esse componente permite que todos usuários iniciem todos os aplicativos. Quando um usuário tenta iniciar um aplicativo que é bloqueado pelas Regras de Controle de Inicialização de Aplicativos, o Kaspersky Endpoint Security impede que esse aplicativo seja iniciado (se a ação **Bloquear** for selecionada) ou salva as informações sobre a inicialização do aplicativo em um relatório (se a ação **Notificar** for selecionada).

Gerenciar as Regras de Controle de Inicialização de Aplicativos

É possível executar as seguintes ações para Regras de Controle de Inicialização de Aplicativos:

- Adicionar nova regra
- Criar ou modificar as condições para acionamento de uma regra
- Editar status da regra

  Uma Regras de Controle de Inicialização de Aplicativos pode ser ativada (a caixa de seleção na frente da regra é marcada) ou desativada (a caixa de seleção na frente da regra é desmarcada). Uma Regra de Controle de Inicialização de Aplicativos é ativada por padrão depois que é criada.
- Excluir regra

Adicionar e editar uma regra de Controle de Inicialização de Aplicativos

Para adicionar ou editar uma regra de Controle de Inicialização de Aplicativos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Inicialização de Aplicativo**.

   Na parte direita da janela, serão exibida as configurações do componente Controle de Inicialização de Aplicativo.
3. Selecione o **Ativar Controle de Inicialização de Aplicativo** para disponibilizar as configurações do componente para edição.
4. Execute uma das seguintes ações:

   - Para adicionar uma regra, clique no botão **Adicionar**.
   - Caso queira editar uma regra existente, selecione-a na lista de regras e clique no botão **Editar**.

   A janela **Regra de Controle de Inicialização de Aplicativos** é exibida.
5. Especificar ou editar as configurações da regra:

   a. No campo **Nome da regra**, insira ou edite o nome da regra.

   b. Na tabela **Condições de Inclusão**, crie ou edite a lista de condições de inclusão que disparam uma regra clicando nos botões **Adicionar**, **Editar**, **Excluir** e **Converter em exclusão**.

c. Na tabela de **Condições de exclusão**, crie ou edite a lista de condições de exclusão que disparam uma regra clicando em **Adicionar**, **Editar**, **Excluir** e **Converter em condição de inclusão**.

d. Se necessário, altere o tipo da condição de acionamento da regra:

- Para alterar o tipo de condição de inclusão para de exclusão, selecione a condição na tabela de **Condições de inclusão** e clique no botão **Converter em exclusão**.
- Para alterar o tipo de condição de exclusão para de inclusão, selecione a condição na tabela de **Condições de exclusão** e clique no botão **Converter em condição de inclusão**.

e. Compile ou edite a lista de usuários e/ou grupos de usuários que têm permissão para executar aplicativos que preenchem as condições de acionamento da regra. Para fazer isto, clique no botão **Adicionar** na tabela **Diretores e seus direitos**.

A janela **Selecionar Usuários ou Grupos**, no Microsoft Windows, abre. Esta janela possibilita selecionar usuários e/ou grupos de usuários.

Por padrão, o valor de **Todos** é adicionado à lista de usuários. A regra aplica-se a todos os usuários.

> Se não houver usuário especificado na tabela, a regra não poderá ser salva.

f. Na tabela **Diretores e seus direitos**, marque as caixas de seleção **Permitir** ou **Bloquear** em frente dos usuários e/ou os grupos dos usuários para determinar o seu direito de iniciar aplicativos.

A caixa de seleção marcada por padrão depende do Modo operacional do Controle de Inicialização de Aplicativo.

g. Marque a caixa de seleção **Negar para outros usuários** se desejar que todos os usuários que não aparecem na coluna **Diretor** e que não são parte do grupo de usuários especificados na coluna **Diretor** sejam bloqueados de iniciar aplicativos que combinam com as condições de acionamento de regra.

> Se a caixa de seleção **Negar para outros usuários** for desmarcada, o Kaspersky Endpoint Security não controlará a inicialização de aplicativos por usuários que não são especificados na tabela **Diretores e seus direitos** e que não pertencem aos grupos de usuários especificados na tabela **Diretores e seus direitos**.

h. Se desejar que o Kaspersky Endpoint Security considere aplicativos que correspondem às condições de acionamento da regra como atualizadores confiáveis para iniciar outros aplicativos para os quais nenhuma regra de Controle de Inicialização de Aplicativos está definida, marque a caixa de seleção **Atualizadores confiáveis**.

6. Clique em **OK**.

7. Para salvar as alterações, clique no botão **Salvar**.

Adicionar uma condição de acionamento a uma regra de Controle de Inicialização de Aplicativos

Para adicionar uma condição de acionamento a uma Regra de Controle de Inicialização de Aplicativos:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Inicialização de Aplicativo**.

   Na parte direita da janela, serão exibida as configurações do componente Controle de Inicialização de Aplicativo.

3. Selecione o **Ativar Controle de Inicialização de Aplicativo** para disponibilizar as configurações do componente para edição.

4. Execute uma das seguintes ações:

   - Se desejar criar uma nova regra e adicionar uma condição de acionamento, clique no botão **Adicionar**.
   - Para adicionar uma condição de acionamento a uma regra existente, selecione a regra na lista de regras e clique no botão **Editar**.

   A janela **Regra de Controle de Inicialização de Aplicativos** é exibida.

5. Na tabela **Condições de inclusão** ou **Condições de exclusão**, clique no botão **Adicionar**.

Você pode usar a lista suspensa do botão **Adicionar** para adicionar várias condições de acionamento à regra (veja as instruções abaixo).

Para adicionar uma condição de acionamento de regra com base nas propriedades dos arquivos na pasta especificada:

1. Na lista suspensa do botão **Adicionar**, selecione **Condição(ões) das propriedades dos arquivos na pasta especificada**.

   A janela **Selecionar pasta**, no Microsoft Windows, é exibida.

2. Na janela **Selecionar pasta**, selecione uma pasta que contenha arquivos de aplicativos executáveis cujas propriedades você deseja utilizar como base para uma ou várias condições de acionamento de uma regra.

3. Clique em **OK**.

   A janela **Adicionar condição** é exibida.

4. Na lista suspensa **Mostrar critérios**, selecione o critério como base no qual você deseja criar uma ou várias condições de acionamento de regra: **Código de hash do arquivo**, **Certificado**, **Categoria KL**, **Metadados** ou **Caminho da pasta**.

   O Kaspersky Endpoint Security não suporta um Código de hash do arquivo MD5 e não controla a inicialização de aplicativos baseados em hash MD5. Um hash SHA256 é usado como uma condição de acionamento da regra.

5. Se você selecionou **Metadados** na lista suspensa **Mostrar critérios**, marque as caixas de seleção do lado oposto a partir de propriedades de arquivo executável que você quer usar na condição de acionamento de regra: **Nome do arquivo**, **Versão do arquivo**, **Nome do aplicativo**, **Versão do aplicativo** e **Fornecedor**.

   Se nenhuma das propriedades especificadas for selecionada, a regra não poderá ser salva.

6. Se você tiver selecionado **Certificado** na lista suspensa **Mostrar critérios**, marque as caixas de seleção aç lado das configurações que você deseja usar na condição de acionamento de regra: **Emissor**, **Diretor** e **Impressão digital**.

   Se nenhuma das configurações especificadas for selecionada, a regra não pode ser salva.

Não se recomenda usar somente os critérios do **Emissor** e **Diretor** como condições de acionamento de regra. O uso desses critérios é inseguro.

7. Marque as caixas de seleção em frente aos nomes dos arquivos executáveis do aplicativo cujas propriedades deseja incluir nas condições de acionamento da regra.

8. Clique no botão **Avançar**.

   Aparece uma lista de formulações de condições de acionamento da regra.

9. Na lista de condições formuladas para acionamento da regra, marque as caixas de seleção opostas às condições de acionamento da regra que deseja adicionar à regra de Controle de Inicialização de Aplicativos.

10. Clique no botão **Encerrar**.

Para adicionar uma condição de acionamento de regra com base nas propriedades dos aplicativos iniciados no computador:

1. Na lista suspensa do botão **Adicionar**, selecione **Condição(ões) das propriedades dos aplicativos iniciados**.

2. Na janela **Adicionar condição**, na lista suspensa **Mostrar critérios** selecione o critério com base no qual você quer criar uma ou várias condições de acionamento de regra: **Código de hash do arquivo**, **Certificado**, **Categoria KL**, **Metadados** ou **Caminho da pasta**.

3. Se você selecionou **Metadados** na lista suspensa **Mostrar critérios**, marque as caixas de seleção do lado oposto a partir de propriedades de arquivo executável que você quer usar na condição de acionamento de regra: **Nome do arquivo**, **Versão do arquivo**, **Nome do aplicativo**, **Versão do aplicativo** e **Fornecedor**.

   Se nenhuma das propriedades especificadas for selecionada, a regra não poderá ser salva.

4. Se você selecionou **Certificado** na lista suspensa **Mostrar critérios**, marque as caixas de seleção diante das configurações que você quer usar na condição de acionamento de regra: **Emissor**, **Diretor**, e **Impressão digital**.

   Se nenhuma das configurações especificadas for selecionada, a regra não pode ser salva.

   Não se recomenda usar somente os critérios do **Emissor** e **Diretor** como condições de acionamento de regra. O uso desses critérios é inseguro.

5. Marque as caixas de seleção em frente aos nomes dos arquivos executáveis do aplicativo cujas propriedades deseja incluir nas condições de acionamento da regra.

6. Clique no botão **Avançar**.

   Aparece uma lista de formulações de condições de acionamento da regra.

7. Na lista de condições formuladas para acionamento da regra, marque as caixas de seleção opostas às condições de acionamento da regra que deseja adicionar à regra de Controle de Inicialização de Aplicativos.

8. Clique no botão **Encerrar**.

Para adicionar uma condição de acionamento de regra com base em uma categoria KL:

1. Na lista suspensa do botão **Adicionar**, selecione **Condições "Categoria KL"**.

   A *Categoria KL* é uma lista de aplicativos que têm atributos de tema compartilhados. A lista é mantida pelos especialistas da Kaspersky. Por exemplo, a Categoria KL de “aplicativos do Office” inclui todos os aplicativos do pacote Microsoft Office, Adobe® Acrobat®, além de outros.

2. Na janela **Condições "Categoria KL"**, selecione as caixas na frente dos nomes daquelas categorias KL com base nas quais você quer criar condições de acionamento de regra.

3. Clique em **OK**.

Para adicionar condições de acionamento de regra personalizadas:

1. Na lista suspensa do botão **Adicionar**, selecione **Condição Personalizada**.

2. Na janela **Condição Personalizada**, clique no botão **Selecionar** e especifique o caminho para o arquivo executável de um aplicativo.

3. Selecionar o critério baseado no qual você deseja criar uma condição de acionamento de regra: **Código de hash do arquivo**, **Certificado**, **Metadados** ou **Caminho para arquivo ou pasta**.

   Se você estiver usando links simbólicos **Caminho para arquivo ou pasta**, você é aconselhado a resolver os links simbólicos para a operação correta da regras de Controle de Inicialização de Aplicativos. Para fazer isso, clique no botão **Resolver link simbólico**.

4. Se necessário, defina as configurações do critério selecionado.

5. Clique em **OK**.

Para adicionar uma condição de acionamento de regra com base em informações sobre a unidade que armazena o arquivo executável de um aplicativo:

1. Na lista suspensa do botão **Adicionar**, selecione **Condição por unidade de arquivo**.

2. Na janela **Condição por unidade de arquivo**, na lista suspensa **Unidade**, selecione o tipo de unidade a partir do qual a inicialização de aplicativos servirá como condição de acionamento de regra.

3. Clique em **OK**.

Alterar o status de uma Regra de Controle de Inicialização de Aplicativos

Para alterar o status de uma regra de Controle de Inicialização de Aplicativos:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Inicialização de Aplicativo**.

   Na parte direita da janela, serão exibida as configurações do componente Controle de Inicialização de Aplicativo.

3. Selecione o **Ativar Controle de Inicialização de Aplicativo** para disponibilizar as configurações do componente para edição.

4. Selecione a regra que deseja editar.

5. Na coluna **Status**, faça o seguinte:

   - Se desejar ativar o uso de uma regra, marque a caixa de seleção ao lado da regra.

- Se desejar desativar o uso de uma regra, desmarque a caixa de seleção ao lado da regra.

6. Para salvar as alterações, clique no botão **Salvar**.

Testando as Regras de Controle de Inicialização de Aplicativos

Para assegurar que as regras de Controle de Inicialização de Aplicativos não bloqueiem aplicativos necessários ao trabalho, recomenda-se colocar as regras recentemente criadas no modo de teste e analisar a sua operação.

Uma análise da operação das Regras de Controle de Inicialização de Aplicativos requer uma revisão dos eventos do Controle de Inicialização de Aplicativo incluídos no relatório do Kaspersky Security Center. Se todos os aplicativos necessários ao trabalho do usuário do computador tiverem permissão para iniciar, significa que as regras foram corretamente criadas. Caso contrário, recomendamos revisar as configurações das regras que você criou.

O modo de teste das Regras de Controle de Inicialização de Aplicativos está desativado por padrão.

Para testar as Regras de Controle de Inicialização de Aplicativos:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Inicialização de Aplicativo**.

   Na parte direita da janela, serão exibida as configurações do componente Controle de Inicialização de Aplicativo.

3. Selecione o **Ativar Controle de Inicialização de Aplicativo** para disponibilizar as configurações do componente para edição.

4. Na lista suspensa **Modo de Controle de Inicialização de Aplicativos**, selecione um dos seguintes itens:

   - **Lista negra**, se você desejar permitir a inicialização de todos os aplicativos, exceto os aplicativos especificados nas regras de bloqueio.

   - **Lista branca**, se você desejar bloquear a inicialização de todos os aplicativos, exceto os aplicativos especificados nas regras de permissão.

5. Na lista suspensa **Ação**, selecione **Notificar**.

6. Para salvar as alterações, clique no botão **Salvar**.

O Kaspersky Endpoint Security não bloqueará aplicativos cuja inicialização é proibida por regras de Controle de Inicialização de Aplicativos, mas enviará notificações sobre a sua inicialização ao Servidor de administração.

Editar os modelos de mensagem do Controle de Inicialização de Aplicativo

Quando um usuário tenta iniciar um aplicativo que está bloqueado por uma regra de Controle de Inicialização de Aplicativos, o Kaspersky Endpoint Security apresenta uma mensagem informando que o aplicativo está bloqueado. Caso o usuário considere que o aplicativo foi bloqueado por engano, o usuário pode utilizar o link no texto da mensagem para enviar uma mensagem ao administrador da rede corporativa local.

Modelos especiais estão disponíveis para a mensagem que é exibida na mensagem ao administrador, quando um aplicativo é bloqueado e não pode iniciar. Você pode modificar os modelos de mensagem.

Para editar um modelo de mensagem:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Inicialização de Aplicativo**.

   Na parte direita da janela, serão exibida as configurações do componente Controle de Inicialização de Aplicativo.
3. Selecione o **Ativar Controle de Inicialização de Aplicativo** para disponibilizar as configurações do componente para edição.
4. Clique no botão **Modelos**.

   A janela **Modelos de mensagem** é exibida.
5. Execute uma das seguintes ações:

   - Se desejar editar o modelo da mensagem que é exibida quando um aplicativo tem o início bloqueado, selecione a guia **Bloqueio**.
   - Se desejar modificar o modelo da mensagem que é enviada ao administrador da rede local, selecione a guia **Mensagem para o administrador**.
6. Modifique o modelo da mensagem que é exibida quando um aplicativo é bloqueado e não pode iniciar ou a mensagem a enviar ao administrador. Para fazer isso, utilize os botões **Padrão** e **Variável**.
7. Clique em **OK**.
8. Para salvar as alterações, clique no botão **Salvar**.

Sobre os modos de funcionamento do Controle de Inicialização de Aplicativo

O componente Controle de Inicialização de Aplicativo funciona em dois modos:

- **Lista negra**. Neste modo, o Controle de Inicialização de Aplicativo permite que todos os usuários iniciem quaisquer aplicativos, exceto aqueles que estão especificados nas regras de bloqueio do Controle de Inicialização de Aplicativo.

  Este modo de Controle de Inicialização de Aplicativo está ativado por padrão.
- **Lista branca**. Neste modo, o Controle de Inicialização de Aplicativo impede que todos os usuários iniciem quaisquer aplicativos, exceto aqueles que estão especificados nas regras de bloqueio do Controle de Inicialização de Aplicativo.

  Quando as regras de permissão do Controle de Inicialização de Aplicativo estão totalmente configuradas, o componente bloqueia o início de todos os novos aplicativos que não foram verificados pelo administrador da rede, ao mesmo tempo em que permite a execução do sistema operacional e de aplicativos confiáveis dos quais os usuários precisam para trabalhar.

Cada modo tem duas ações que podem ser tomadas nos aplicativos em execução: o Kaspersky Endpoint Security pode bloquear a inicialização dos aplicativos ou notificar o usuário sobre a inicialização de um aplicativo que coincide com as condições das Regras de Controle de Inicialização de Aplicativos.

O Controle de Inicialização de Aplicativo pode ser configurado para ser executado nestes dois modos, usando a interface local do Kaspersky Endpoint Security e usando o Kaspersky Security Center.

Contudo, o Kaspersky Security Center oferece ferramentas que não estão disponíveis na interface local do Kaspersky Endpoint Security, como as ferramentas que são necessárias para as seguintes tarefas:

- Criar categorias do aplicativo.

  As Regras de Controle de Inicialização de Aplicativos criadas no Console de Administração do Kaspersky Security Center são baseadas em categorias de aplicativos personalizados e não nas condições de inclusão e exclusão, como é o caso da interface local do Kaspersky Endpoint Security.

- Coletar informações sobre aplicativos que estão instalados em computadores da rede.

É por isso que se recomenda usar o Kaspersky Security Center para configurar a operação do componente Controle de Inicialização de Aplicativo.

Selecionar o modo do Controle de Inicialização de Aplicativos

Para selecionar o modo de Controle de Inicialização de Aplicativos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Inicialização de Aplicativo**.

   Na parte direita da janela, serão exibida as configurações do componente Controle de Inicialização de Aplicativo.
3. Selecione o **Ativar Controle de Inicialização de Aplicativo** para disponibilizar as configurações do componente para edição.
4. Na lista suspensa **Modo de Controle de Inicialização de Aplicativos**, selecione uma das seguintes opções:

   - **Lista negra**, se você desejar permitir a inicialização de todos os aplicativos, exceto os aplicativos especificados nas regras de bloqueio.
   - **Lista branca**, se você desejar bloquear a inicialização de todos os aplicativos, exceto os aplicativos especificados nas regras de permissão.

     Quando esse modo é selecionado, duas Regras de Controle de Inicialização de Aplicativos são criadas por padrão: **Golden Image** e **Atualizadores confiáveis**. Você não é possível excluir essas regras. As configurações dessas regras não podem ser editadas. Você pode ativar ou desativar essas regras marcando ou desmarcando a caixa de seleção na frente da regra relevante. Por padrão, a regra **Golden Image** é ativada, e a regra **Atualizadores confiáveis** é desativada. Todos os usuários podem iniciar aplicativos que combinam com as condições de acionamento dessas regras.

   Todas as regras criadas durante o modo selecionado são salvas depois que o modo é modificado, para que as regras possam ser usadas novamente. Para reverter para o uso dessas regras, tudo que você tem que fazer é selecionar o modo necessário na lista suspensa **Modo de Controle de Inicialização de Aplicativos**.
5. Na lista suspensa **Ação**, selecione a ação a ser executada pelo componente quando um usuário tenta iniciar um aplicativo que é bloqueado pelas Regras de Controle de Inicialização de Aplicativos.

6. Marque a caixa de seleção **Monitorar DLL e drivers** se você desejar que o Kaspersky Endpoint Security controle o carregamento de módulos DLL quando os aplicativos são iniciados pelos usuários.

   As informações sobre o módulo e o aplicativo que carregou o módulo serão salvas em um relatório.

   Se a caixa de seleção for marcada, os módulos e drivers DLL serão monitorados antes que o Kaspersky Endpoint Security seja iniciado. Para configurar a monitorização subsequente de todos os drivers e módulos DLL antes da inicialização do aplicativo, reinicie o computador depois de marcar caixa **Monitorar DLL e drivers**. Se você não conseguir reiniciar o computador, depois de marcar a caixa de seleção **Monitorar DLL e drivers**, você pode carregar os módulos DLL e drivers enquanto o Kaspersky Endpoint Security estiver em execução. Nesta caixa, a monitorização só entra em vigor para módulos DLL e drivers que são carregados enquanto o Kaspersky Endpoint Security está em execução.

   Ao monitorar módulos DLL e drivers, não é recomendável usar regras de Controle de Inicialização de Aplicativos que foram criadas baseadas em categorias KL. A determinação de categorias KL (inclusive nas regras "Sistema operacional e os seus componentes") para módulos DLL e drivers pode não funcionar corretamente. Especificamente, a regra "Sistema operacional e os seus componentes" regra foi criada por padrão e não é distribuída no módulo DLL e na inicialização do driver. Ao ativar esta função, é necessário criar regras de permissão separadas para módulos DLL e drivers. Usar a função **Controlar DLL e drivers** se tais regras de permissão não existirem pode tornar o sistema instável.

   Recomendamos que a proteção por senha seja ativada para definir as configurações do programa para que seja possível desativar as regras de permissão que bloqueiam a inicialização de módulos DLL e drivers criticamente importantes, sem modificar as configurações de política do Kaspersky Security Center no processo.

7. Para salvar as alterações, clique no botão **Salvar**.

Gerenciar as regras de Controle de Inicialização de Aplicativos usando o Kaspersky Security Center

Esta seção contém informações sobre a utilização do Kaspersky Security Center para configurar Regras de Controle de Inicialização de Aplicativos e fornece recomendações sobre o uso ideal do Controle de Inicialização de Aplicativos.

Coletar informações sobre aplicativos que estão instalados no computador de usuários

Para criar ótimas Regras de Controle de Inicialização de Aplicativos, recomenda-se primeiro obter um quadro dos aplicativos que são usados nos computadores na rede local. Para fazer isto, você pode obter as seguintes informações:

- Fornecedores, versões e localizações de aplicativos usados na rede corporativa.
- Frequência das atualizações do aplicativo.
- As políticas de uso de aplicativo adotadas na empresa (pode ser políticas de segurança ou políticas administrativas).

- Localização do armazenamento dos pacotes de distribuição do aplicativo.

As informações sobre aplicativos que são usados em computadores na rede local estão disponíveis na pasta **Registro de aplicativos** e na pasta de **Arquivos executáveis**. A pasta **Registros de aplicativos** e a pasta **Arquivos executáveis** estão na pasta **Gerenciamento do aplicativo** na árvore do Console de Administração do Kaspersky Security Center.

A pasta **Aplicativos do registro** contém a lista de aplicativos que foram detectados pelo Agente de Rede instalado no computador cliente.

A pasta **Arquivos executáveis** contém uma lista de todos os arquivos executáveis que foram alguma vez iniciados em computadores de cliente ou que foram detectados durante a tarefa de inventário do Kaspersky Endpoint Security.

Para visualizar informações gerais sobre o aplicativo e os respectivos arquivos executáveis, e a lista de computadores em que o aplicativo está instalado, abra a janela propriedades do aplicativo que está selecionada na pasta **Aplicativos do registro** ou na pasta **Arquivos executáveis**.

Criar categorias do aplicativo

Para mais conveniência ao criar regras, você pode criar categorias de aplicativos e usá-las ao criar Regras de Controle de Inicialização de Aplicativos.

É recomendável criar a categoria "Aplicativos de trabalho" que abrange o conjunto de aplicativos padrão que é usado pela empresa. Se diferentes grupo de usuários usam conjuntos de aplicativos diversos, é possível criar uma categoria de aplicativos separada para cada grupo de usuários.

Para criar uma categoria de aplicativos:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do Console de Administração, selecione a pasta **Adicional** → **Gerenciamento de aplicativo** → **Categorias de Aplicativo**.
3. Clique no botão **Criar categoria** no espaço de trabalho.

   O assistente de criação de categoria de usuário é iniciado.
4. Siga as instruções do assistente de criação de categoria de usuário.

Criar Regras de Controle de Inicialização de Aplicativos usando o Kaspersky Security Center

Para criar uma Regra de Controle de Inicialização de Aplicativos usando o Kaspersky Security Center:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Controle de Endpoints**, selecione a subseção **Controle de Inicialização de Aplicativo**.

   Na parte direita da janela, serão exibida as configurações do componente Controle de Inicialização de Aplicativo.

7. Clique no botão **Adicionar**.

   A janela **Regra de Controle de Inicialização de Aplicativos** é exibida.

8. Na lista suspensa **Categoria**, selecione a categoria de aplicativo criada com base na qual você deseja criar uma regra.

9. Especifique a lista de usuários e/ou grupos de usuários aos quais deseja permissão para iniciar os aplicativos da categoria selecionada. Para fazer isto, na tabela **Diretores e seus direitos**, clique no botão **Adicionar**.

   A janela padrão **Selecionar Usuários ou Grupos**, no Microsoft Windows, abre. Esta janela possibilita selecionar usuários e/ou grupos de usuários.

10. Na tabela **Diretores e seus direitos**:

    - Se desejar permitir que os usuários e/ou grupos dos usuários iniciem aplicativos que pertencem à categoria selecionada, marque as caixas de seleção **Permitir** ao lado desse usuários.
    - Se desejar impedir que os usuários e/ou grupos dos usuários iniciem aplicativos que pertencem à categoria selecionada, marque as caixas de seleção **Bloquear** ao lado desses usuários.

11. Marque a caixa de seleção **Negar para outros usuários** se desejar que todos os usuários que não aparecem na coluna **Diretor** e que não fazem parte do grupo de usuários especificados na coluna **Diretor** sejam bloqueados de iniciarem aplicativos que pertencem à categoria selecionada.

12. Se desejar que o Kaspersky Endpoint Security inclua aplicativos da categoria que está especificada na regra como atualizadores confiáveis, com o direito de iniciarem outros aplicativos para os quais nenhuma Regra de Controle de Inicialização de Aplicativos está definida, marque a caixa de seleção **Atualizadores confiáveis**.

13. Clique em **OK**.

14. Na seção **Controle de Inicialização de Aplicativo** da janela de propriedades da política, clique no botão **Aplicar**.

Alterar o status de uma Regra de Controle de Inicialização de Aplicativos usando o Kaspersky Security Center

Para alterar o status de uma regra de Controle de Inicialização de Aplicativos:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Controle de Endpoints**, selecione a subseção **Controle de Inicialização de Aplicativo**.

   Na parte direita da janela, serão exibida as configurações do componente Controle de Inicialização de Aplicativo.

7. Selecione a Regra de Controle de Inicialização de Aplicativos cujo status desejar alterar.

8. Na seção **Status**, execute uma das seguintes operações:

   - Se desejar ativar o uso de uma regra, marque a caixa de seleção ao lado da regra.
   - Se desejar desativar o uso de uma regra, desmarque a caixa de seleção ao lado da regra.

9. Clique no botão **Aplicar**.

Controle de Privilégios de Aplicativo

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado com o Microsoft Windows para estações de trabalho. Este componente estará indisponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado no Microsoft Windows para servidores de arquivos.

Esta seção contém informações sobre o Controle de Privilégios de Aplicativo e instruções sobre como definir as configurações do componente.

Sobre o Controle de Privilégios de Aplicativo

O Controle de Privilégios de Aplicativo impede que os aplicativos executem ações perigosas para o sistema, e assegura o controle de acesso aos recursos do sistema operacional e aos dados de identidade.

Este componente controla a atividade dos aplicativos, incluindo o acesso a recursos protegidos (como arquivos e pastas, chaves de registro), através das *regras de controle de aplicativos*. As regras de controle de aplicativos são um conjunto de restrições que se aplicam a várias ações de aplicativos do sistema operacional e aos direitos de acesso aos recursos do sistema.

A atividade de rede dos aplicativos é monitorada pelo componente Firewall.

Ao iniciar o aplicativo pela primeira vez, o Controle de Privilégios de Aplicativo verifica o aplicativo e o coloca em um grupo confiável. O grupo confiável define as regras de controle de aplicativos que o Kaspersky Endpoint Security aplica quando controla a atividade do aplicativo.

Recomendamos que você participe do Kaspersky Security Network para tornar o trabalho de Controle de Privilégio de Aplicativo mais eficiente. Os dados obtidos através do Kaspersky Security Network permitem classificar os aplicativos em grupos com exatidão e aplicar as melhores regras de controle de aplicativos.

Na próxima vez em que o aplicativo for iniciado, o Controle de Privilégios de Aplicativo verifica a integridade do aplicativo. Se o aplicativo não tiver sofrido alterações, o componente aplicará as regras de controle de aplicativos atuais. Caso tenham existido alterações no aplicativo, o Controle de Privilégios de Aplicativo verifica-o novamente, como se estivesse sendo iniciado pela primeira vez.

Limitações do controle de dispositivo de áudio e vídeo

Sobre a proteção de fluxo de áudio

A proteção de fluxo de áudio tem as seguintes considerações especiais:

- O componente Controle de Privilégios de Aplicativo deve estar ativado para esta funcionalidade funcionar.
- Se o aplicativo começou a receber o fluxo de áudio antes que o componente de Controle de Privilégios de Aplicativo fosse iniciado, o Kaspersky Endpoint Security permitirá ao aplicativo receber o fluxo de áudio e não mostrará nenhuma notificação.

- Se você moveu o aplicativo para o grupo **Não confiável** ou o grupo de **Alta restrição** depois que o aplicativo começou a receber o fluxo de áudio, o Kaspersky Endpoint Security permite ao aplicativo receber o fluxo de áudio e não mostra nenhuma notificação.

- Depois que as configurações do acesso a aplicativo a dispositivos de gravação de som foram modificadas (por exemplo, se o aplicativo foi bloqueado de receber o fluxo de áudio na janela de configurações do Controle de aplicativos), este aplicativo deve ser reiniciado para parar de receber o fluxo de áudio.

- O controle do acesso ao fluxo de áudio de dispositivos de gravação de som não depende de configurações de acesso à câmara da Web de um aplicativo.

- O Kaspersky Endpoint Security protege o acesso somente a microfones integrados e microfones externos. Outros dispositivos de transmissão de áudio não são suportados.

- O Kaspersky Endpoint Security não pode garantir a proteção de um fluxo de áudio de tais dispositivos como câmeras DSLR, câmeras de vídeo portáteis, e câmeras de ação.

Considerações especiais da operação de dispositivos áudio e vídeo durante a instalação e a atualização do Kaspersky Endpoint Security

Quando você executa aplicativos de reprodução ou gravação de áudio e vídeo pela primeira vez, desde a instalação do Kaspersky Endpoint Security, a reprodução áudio e vídeo ou gravação pode ser interrompida. Isto é necessário para ativar a funcionalidade que controla o acesso a dispositivos de gravação de som por aplicativos. O serviço do sistema que controla o hardware áudio será reiniciado quando o Kaspersky Endpoint Security for executado pela primeira vez.

Sobre acesso a webcams por aplicativos

A funcionalidade de proteção de acesso à webcam tem as seguintes considerações especiais e limitações:

- O aplicativo controla vídeo e imagens estáticas derivadas do processamento de dados da webcam.

- O aplicativo controla o fluxo de áudio se ele for parte do fluxo vídeo recebido da webcam.

- O aplicativo controla somente webcams conectadas via USB ou IEEE1394 que são exibidos como **Dispositivos de imagem** no Gerenciador de Dispositivo do Windows.

Webcams suportadas

Kaspersky Endpoint Security suporta as seguintes webcams:

- Logitech HD Webcam C270

- Logitech HD Webcam C310

- Logitech Webcam C210

- Logitech Webcam Pro 9000

- Logitech HD Webcam C525

- Microsoft LifeCam VX-1000

- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

A Kaspersky não pode garantir o suporte de webcams que não estão especificadas nessa lista.

Ativar e desativar o Controle de Privilégios de Aplicativo

Por padrão, o Controle de Privilégios de Aplicativo está ativado e é executado no modo recomendado pelos especialistas da Kaspersky. É possível desativar o Controle de Privilégios de Aplicativo, se necessário.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

Para ativar ou desativar o Controle de Privilégios de Aplicativo na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Controle de Endpoints**.

   A seção **Controle de Endpoints** é exibida.
4. Clique com o botão direito do mouse para exibir o menu de contexto da linha com as informações sobre o componente Controle de Privilégios de Aplicativo.

   Será aberto um menu para a seleção de ações.
5. Execute uma das seguintes ações:

   - Para ativar o Controle de Privilégios de Aplicativo, selecione **Iniciar**.

     O ícone de status do componente , exibido à esquerda, na linha do Controle de Privilégios de Aplicativo, muda para o ícone .
   - Para desativar o componente Controle de Privilégios de Aplicativo, selecione **Interromper**.

     O ícone de status do componente , exibido à esquerda, na linha do Controle de Privilégios de Aplicativo, muda para o ícone .

Para ativar ou desativar o Controle de Privilégios de Aplicativo na janela de configuração do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.

3. Na parte direita da janela, execute uma das seguintes operações:

   - Para ativar o Controle de Privilégios de Aplicativo, marque a caixa de seleção **Ativar Controle de Privilégios de Aplicativo**.
   - Para desativar o Controle de Privilégios de Aplicativo, desmarque a caixa de seleção **Ativar Controle de Privilégios de Aplicativo**.

4. Para salvar as alterações, clique no botão **Salvar**.

Gerenciar grupos confiáveis de aplicativos

Ao iniciar o aplicativo pela primeira vez, o componente Controle de Privilégios de Aplicativo verifica a segurança e coloca esse aplicativo em um grupo confiável.

Na primeira etapa da verificação do aplicativo, o Kaspersky Endpoint Security verifica o banco de dados interno de aplicativos conhecidos para detectar uma entrada correspondente e, simultaneamente, envia uma solicitação ao banco de dados do Kaspersky Security Network (se houver uma conexão com a Internet). De acordo com os resultados da pesquisa no banco de dados interno e o banco de dados do Kaspersky Security Network, o aplicativo é colocado em um grupo confiável. Cada vez que o aplicativo é iniciado, o Kaspersky Endpoint Security envia uma nova pergunta ao banco de dados do KSN e coloca o aplicativo em um grupo confiável diferente, se a reputação do aplicativo nos bancos de dados da KSN tiver sido modificada.

Você pode selecionar um grupo de confiança ao qual o Kaspersky Endpoint Security atribui automaticamente todos os aplicativos desconhecidos. Os aplicativos que foram iniciados antes do Kaspersky Endpoint Security são automaticamente movidos para o grupo confiável especificado na janela **Selecionar grupo confiável**.

O componente controla somente a atividade de rede de aplicativos iniciados antes do Kaspersky Endpoint Security com base no conjunto de regras de rede nas configurações de Firewall.

Configurar as definições para atribuir aplicativos a grupos confiáveis

Se a participação no Kaspersky Security Network for ativada, o Kaspersky Endpoint Security enviará ao KSN uma consulta sobre a reputação de um aplicativo cada vez que o aplicativo for iniciado. Com base na resposta do KSN, o aplicativo pode ser movido para um grupo confiável diferente daquele especificado nas configurações do Controle de Privilégios de Aplicativo.

Para definir as configurações para colocar os aplicativos em um grupo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.

3. Se desejar colocar automaticamente aplicativos com assinatura digital de fornecedores confiáveis no grupo Confiáveis, marque a caixa de seleção **Confiar em aplicativos com assinatura digital**.

Fornecedores confiáveis são aqueles fornecedores incluídos no grupo de confiança pela Kaspersky. Também é possível adicionar certificados de fornecedores manualmente ao armazenamento de certificados do sistema confiável.

4. Escolha como deseja que os aplicativos desconhecidos sejam atribuídos aos grupos de confiança:

   - Para usar a análise heurística para atribuir aplicativos desconhecidos a grupos confiáveis, selecione a opção **Usar a análise heurística para definir o grupo** e especifique o período de tempo alocado para verificar o aplicativo iniciado no campo **Tempo máximo para definir grupo**.
   - Se desejar atribuir todos os aplicativos desconhecidos a um grupo confiável especificado, selecione a opção **Mover automaticamente para o grupo** e selecione o grupo confiável desejado na lista suspensa.

     Para fins de segurança, o grupo **Confiáveis** não é incluído nos valores da configuração **Mover automaticamente para o grupo**.

5. Para salvar as alterações, clique no botão **Salvar**.

Modificar um grupo confiável

Ao iniciar o aplicativo pela primeira vez, o Kaspersky Endpoint Security o coloca em um grupo confiável automaticamente. É possível mover o aplicativo para outro grupo de confiança manualmente, se necessário.

Os especialistas da Kaspersky não recomendam mover os aplicativos que foram atribuídos automaticamente a um grupo de confiança para outro. Em vez disso, você pode editar as regras de um aplicativo individual.

Para alterar o grupo de confiança atribuído ao aplicativo automaticamente pelo Kaspersky Endpoint Security ao ser iniciado pela primeira vez:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.
3. Clique no botão **Aplicativos**.

   A guia **Regras de Controle de Aplicativos** na janela **Aplicativos** é aberta.
4. Selecione o aplicativo relevante na guia **Regras de Controle de Aplicativos**.
5. Execute uma das seguintes ações:

   - Clique com o botão direito para exibir o menu de contexto do aplicativo. No menu de contexto do aplicativo, selecione **Mover para o grupo→ <nome do grupo>**.
   - Para abrir o menu de contexto, clique no link **Confiáveis** / **Baixa restrição** / **Alta restrição** / **Não confiável**. No menu de contexto, selecione o grupo confiável desejado.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Selecionar um grupo confiável de aplicativos iniciados antes do Kaspersky Endpoint Security

O componente controla somente a atividade de rede de aplicativos que foram iniciados antes do Kaspersky Endpoint Security. O controle é executado segundo as regras de rede especificadas nas configurações de Firewall. Para especificar que regras de rede devem ser aplicadas à monitorização de atividade de rede de tais aplicativos, você deve selecionar um grupo confiável.

Para selecionar o grupo confiável de aplicativos iniciados antes do Kaspersky Endpoint Security:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.
3. Clique no botão **Editar**.

   Isto abre a janela **Selecionar grupo confiável**.
4. Selecione o grupo confiável necessário.
5. Clique em **OK**.
6. Para salvar as alterações, clique no botão **Salvar**.

Gerenciar as regras de controle de aplicativos

Por padrão, a atividade de aplicativos é monitorada por regras de controle de aplicativos que são definidas para o grupo de confiança de atribuição do aplicativo pelo Kaspersky Endpoint Security na primeira vez que é iniciado. Se necessário, você pode editar as configurações das regras de controle de aplicativos para todo o grupo de confiança, para um aplicativo individual ou para um grupo de aplicativos sob um grupo de confiança.

As regras de controle de aplicativos definidas para aplicativos individuais ou grupos de aplicativos sob um grupo de confiança têm prioridade sobre regras de controle de aplicativos que são definidas para um grupo de confiança. Em outras palavras, se as configurações das regras de controle de aplicativos para um aplicativo individual ou um grupo de aplicativos em um grupo confiável diferirem das configurações das regras de controle de aplicativos definidas para o grupo confiável, o componente Controle de Privilégios de Aplicativo monitora a atividade do aplicativo ou grupo de aplicativos no grupo confiável segundo as regras de controle de aplicativos que são para o aplicativo ou o grupo de aplicativos.

Alterar regras de controle de aplicativos para grupos confiáveis e grupos de aplicativos

A otimização das regras de controle de aplicativos para diferentes grupos de confiança são criadas por padrão. As configurações de regras para controle de grupo de aplicativos herdam valores das configurações das regras do controle de grupo de confiança. Você pode editar as regras do controle de grupo de confiança e as regras para controle de grupo de aplicativos predefinidas.

Para editar as regras do controle de grupo de confiança e as regras para controle de grupo de aplicativos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.
3. Clique no botão **Aplicativos**.

   É exibida a guia de **Regras de Controle de Aplicativos** na janela **Controle de Privilégios de Aplicativo**.
4. Selecione o grupo confiável necessário ou grupo de aplicativos.
5. No menu de contexto do grupo confiável ou grupo de aplicativos, selecione **Regras de grupos**.

   A janela **Regras de Controle do grupo de aplicativos** abre.
6. Na janela **Regras de Controle do grupo de aplicativos**, execute uma das seguintes operações:

   - Para editar as regras de controle do grupo confiável ou as regras de controle do grupo de aplicativos que regem os direitos do grupo confiável ou do grupo de aplicativos para acessar o registro do sistema operacional, os arquivos do usuário e as configurações do aplicativo, selecione a guia **Registro do sistema e arquivos**.
   - Para editar as regras de controle do grupo confiável ou as regras de controle do grupo de aplicativos que regem os direitos do grupo confiável ou do grupo de aplicativos para acessar os processos e objetos do sistema operacional, selecione a guia **Direitos**.
7. No recurso desejado, na coluna da ação correspondente, clique com o botão direito do mouse para abrir o menu de contexto.
8. No menu de contexto, selecione o item desejado.

   - **Herdar**
   - **Permitir**
   - **Bloquear**
   - **Registrar eventos**

   Se estiver editando regras do controle de grupo de confiança, o item **Herdar** não estará disponível.
9. Clique em **OK**.
10. Na janela **Aplicativos**, clique em **OK**.
11. Para salvar as alterações, clique no botão **Salvar**.

Editar uma regra de controle de aplicativos

Por padrão, as configurações de regras de controle de aplicativos daqueles que pertencem a um grupo de aplicativos ou de confiança herdam os valores das configurações de regras do controle de grupo de confiança. Você pode editar as configurações das regras de controle de aplicativos.

Para alterar uma regra do controle de aplicativos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.
3. Clique no botão **Aplicativos**.

   É exibida a guia de **Regras de Controle de Aplicativos** na janela **Controle de Privilégios de Aplicativo**.
4. Selecione o aplicativo desejado.
5. Execute uma das seguintes ações:

   - No menu de contexto do aplicativo, selecione **Regras de Aplicativo**.
   - Clique no botão **Adicional** no canto inferior direito da guia **Regras de controle de aplicativos**.

   A janela **Regras de Controle de Aplicativos** abre.
6. Na janela **Regras de Controle de Aplicativos** execute uma das seguintes operações:

   - Para editar as regras de controle de aplicativos que regem os direitos do aplicativo para acessar o registro do sistema operacional, arquivos do usuário e configurações do aplicativo, selecione a guia **Registro do sistema e arquivos**.
   - Para editar as regras de controle de aplicativos que regem os direitos do aplicativo para acessar os processos e objetos do sistema operacional, selecione a guia **Direitos**.
7. No recurso desejado, na coluna da ação correspondente, clique com o botão direito do mouse para abrir o menu de contexto.
8. No menu de contexto, selecione o item desejado.

   - **Herdar**
   - **Permitir**
   - **Bloquear**
   - **Registrar eventos**
9. Clique em **OK**.
10. Na janela **Aplicativos**, clique em **OK**.

11. Para salvar as alterações, clique no botão **Salvar**.

Desativar downloads e atualizações de regras de controle de aplicativos no banco de dados do Kaspersky Security Network

Por padrão, quando as novas informações sobre um aplicativo são detectadas no banco de dados do Kaspersky Security Network, o Kaspersky Endpoint Security aplica as regras de controle baixadas do banco de dados KSN nesse aplicativo. Em seguida, você pode editar manualmente as regras de controle do aplicativo.

Se o aplicativo não estava no banco de dados do Kaspersky Security Network quando foi iniciado pela primeira vez, mas as informações sobre este foram adicionadas ao banco de dados posteriormente, por padrão o Kaspersky Endpoint Security atualiza automaticamente as regras de controle para esse aplicativo.

Você pode desativar o download de regras de controle de aplicativos e as atualizações automáticas de regras de controle de aplicativos desconhecidas anteriormente no banco de dados do Kaspersky Security Network.

Para desativar o download e as atualizações de regras de controle de aplicativos no banco de dados do Kaspersky Security Network:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.
3. Desmarque a caixa de seleção **Atualizar regras de controle para aplicativos anteriormente desconhecidos dos bancos de dados da KSN**.
4. Para salvar as alterações, clique no botão **Salvar**.

Desativar a herança de restrições do processo pai

A inicialização do aplicativo pode ser executada pelo usuário ou por outro aplicativo em execução. Quando a inicialização do aplicativo é executada por outro aplicativo, será criado um procedimento de inicialização, que consiste de processos aplicativos pai e filho.

Quando um aplicativo tenta obter acesso a um recurso protegido, o Controle de Privilégios de Aplicativo analisa todos os processos pai do aplicativo para determinar se estes processos têm direitos para acessar o recurso protegido. A regra de prioridade mínima é então observada: ao comparar os direitos de acesso do aplicativo àqueles dos processos pai, são aplicados os direitos de acesso de prioridade mínima à atividade do aplicativo.

A prioridade dos direitos de acesso dá-se da seguinte forma:

1. **Permitir** Este direito de acesso têm a prioridade mais alta.
2. **Bloquear** Este direito de acesso têm a prioridade mais baixa.

Este mecanismo evita que um aplicativo não confiável ou com direitos restritos use um aplicativo confiável para executar ações que exigem privilégios determinados.

Se a atividade de um aplicativo for bloqueada devido à falta de direitos que são concedidos a um processo pai, você pode editar estes direitos ou desativar a herança de restrições do processo pai.

Para desativar a herança de restrições do processo pai:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.
3. Clique no botão **Aplicativos**.

   É exibida a guia de **Regras de Controle de Aplicativos** na janela **Controle de Privilégios de Aplicativo**.
4. Selecione o aplicativo desejado.
5. No menu de contexto do aplicativo, selecione **Regras de Aplicativo**.

   A janela **Regras de Controle de Aplicativos** abre.
6. Na janela **Regras de Controle de Aplicativos**, selecione a guia **Exclusões**.
7. Marque a caixa de seleção **Não herdar restrições do processo principal (aplicativo)**.
8. Clique em **OK**.
9. Na janela **Aplicativos**, clique em **OK**.
10. Para salvar as alterações, clique no botão **Salvar**.

Excluir ações específicas do aplicativo das regras de controle de aplicativos

Para excluir ações específicas do aplicativo das regras de controle de aplicativos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.
3. Clique no botão **Aplicativos**.

   É exibida a guia de **Regras de Controle de Aplicativos** na janela **Controle de Privilégios de Aplicativo**.
4. Selecione o aplicativo desejado.
5. No menu de contexto do aplicativo, selecione **Regras de Aplicativo**.

   A janela **Regras de Controle de Aplicativos** abre.
6. Selecione a guia **Exclusões**.
7. Marque as caixas de seleção ao lado das ações do aplicativo que não precisam ser monitoradas.

8. Clique em **OK**.
9. Na janela **Aplicativos**, clique em **OK**.
10. Para salvar as alterações, clique no botão **Salvar**.

Remover regras de controle de aplicativos desatualizadas

Por padrão, as regras do controle de aplicativos que não foram executados em 60 dias são excluídas automaticamente. Você pode modificar o tempo de armazenamento de regras do controle de aplicativos não utilizados ou ativar a exclusão automática de regras.

Para excluir regras de controle de aplicativos antigas:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.
3. Execute uma das seguintes ações:

   - Para que o Kaspersky Endpoint Security exclua regras do controle de aplicativos não utilizados, selecione a caixa de seleção **Excluir regras para aplicativos não executados por mais de** e especifique o número de dias desejado.
   - Para desativar a exclusão automática de regras do controle de aplicativos não utilizados, desmarque a caixa de seleção **Excluir regras para aplicativos não executados por mais de**.
4. Para salvar as alterações, clique no botão **Salvar**.

Proteger os recursos e dados de identidade do sistema operacional

O Controle de Privilégios de Aplicativo gerencia os direitos de ação em várias categorias de recursos e dados de identidade do sistema operacional.

Os especialistas da Kaspersky criaram categorias predefinidas de recursos protegidos. As categorias predefinidas de recursos protegidos ou as categorias de recursos protegidos sob estas categorias não podem ser editadas ou excluídas.

É possível executar as seguintes ações:

- Adicionar uma nova categoria de recursos protegidos.
- Adicionar um novo recurso protegido.
- Desativar a proteção de um recurso.

Adicionar uma categoria de recursos protegidos

Para adicionar uma nova categoria ou recursos protegidos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.
3. Clique no botão **Recursos**.

   É exibida a guia **Recursos protegidos** na janela **Controle de Privilégios de Aplicativo**.
4. Na parte esquerda da guia **Recursos protegidos**, selecione uma seção ou categoria ou recursos protegidos para a qual você pretende adicionar uma nova categoria ou recursos protegidos.
5. Clique no botão **Adicionar** e na lista suspensa selecione **Categoria**.

   A janela **Categoria de recursos protegidos** é aberta.
6. Na janela **Categoria ou recursos protegidos** que se abriu, insira um nome para a nova categoria ou recursos protegidos.
7. Clique em **OK**.

   Um novo item é exibido na lista de categorias de recursos protegidos.
8. Na janela **Controle de Privilégios de Aplicativo**, clique em **OK**.
9. Para salvar as alterações, clique no botão **Salvar**.

Depois de adicionar a categoria ou recursos protegidos, é possível editá-la ou removê-la clicando nos botões **Editar** ou **Remover** na parte superior esquerda da guia **Recursos protegidos**.

Adicionar um recurso protegido

Para adicionar um recurso protegido:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.
3. Clique no botão **Recursos**.

   É exibida a guia **Recursos protegidos** na janela **Controle de Privilégios de Aplicativo**.
4. Na parte esquerda da guia **Recursos protegidos**, selecione a categoria ou recursos protegidos para a qual você pretende adicionar um novo recurso protegido.

5. Clicar no botão **Adicionar** e na lista suspensa selecione o tipo do recurso que você quer adicionar:

   - **Arquivo ou pasta**.
   - **Chave do Registro**.

   A janela **Recurso protegido** é aberta.

6. Na janela **Recurso protegido**, insira o nome do recurso protegido no campo **Nome**.
7. Clique no botão **Procurar**.
8. Na janela que se abriu, especifique as configurações necessárias dependendo do tipo de recurso protegido que você pretende adicionar. Clique em **OK**.
9. Na janela **Recurso protegido**, clique em **OK**.

   Um novo item é exibido na lista de recursos protegidos da categoria marcada na guia **Recursos protegidos**.

10. Na janela **Controle de Privilégios de Aplicativo**, clique em **OK**.
11. Para salvar as alterações, clique no botão **Salvar**.

Depois de adicionar um recurso protegido, é possível editá-lo ou removê-lo clicando nos botões **Editar** e **Remover** na parte superior esquerda da guia **Recursos protegidos**.

Desativar a proteção de recursos

Para desativar a proteção de recursos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Privilégios de Aplicativo**.

   Na parte direita da janela, as configurações do componente Controle de Privilégios de Aplicativo são exibidas.

3. Na parte direita da janela, clique no botão **Recursos**.

   É exibida a guia **Recursos protegidos** na janela **Controle de Privilégios de Aplicativo**.

4. Execute uma das seguintes ações:

   - Na parte esquerda da guia, na lista de recursos protegidos, selecione o recurso para o qual deseja desativar a proteção e desmarque a caixa de seleção próxima do nome deste.
   - Clique em **Exclusões** e faça o seguinte:

     a. No janela **Exclusões**, clique no botão **Adicionar**. Na lista suspensa, selecione o tipo de recurso que deseja adicionar à lista de exclusões da proteção pelo componente Controle de Privilégios de Aplicativo: (**Arquivo ou pasta** ou **Chave do registro**).

     A janela **Recurso protegido** é aberta.

     b. Na janela **Recurso protegido**, insira o nome do recurso protegido no campo **Nome**.

c. Clique no botão **Procurar**.

d. Na janela que se abriu, especifique as configurações desejadas, de acordo com o tipo de recurso protegido que você pretende adicionar à lista de exclusões da proteção pelo componente Controle de Privilégios de Aplicativo.

e. Clique em **OK**.

f. Na janela **Recurso protegido**, clique em **OK**.

É exibido um novo elemento na lista de recursos que estão excluídos da proteção pelo componente Controle de Privilégios de Aplicativo.

> Depois de adicionar um recurso à lista de exclusões da proteção pelo componente Controle de Privilégios de Aplicativo, é possível editá-lo ou removê-lo clicando nos botões **Editar** ou **Remover**na parte superior da janela **Exclusões**.

g. Na janela **Exclusões**, clique em **OK**.

5. Na janela **Controle de Privilégios de Aplicativo**, clique em **OK**.

6. Para salvar as alterações, clique no botão **Salvar**.

Monitoramento de Vulnerabilidades

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado com o Microsoft Windows para estações de trabalho. Este componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que esteja executando o Microsoft Windows para servidores de arquivos.

Esta seção contém informações sobre Monitoramento de Vulnerabilidades e instruções sobre como ativar ou desativar o componente.

Sobre o Monitoramento de Vulnerabilidades

O componente Monitoramento de vulnerabilidades executa a verificação de vulnerabilidades em tempo real de aplicativos em execução no computador do usuário e iniciados por ele. Quando o componente Monitoramento de Vulnerabilidades está ativo, não é necessário iniciar a tarefa de Verificação de Vulnerabilidades. Esta verificação é relevante se a tarefa de Verificação de Vulnerabilidades de aplicativos que foram instalados no computador do usuário nunca tiver sido executada ou tiver sido executada há muito tempo.

Ativar e desativar o Monitoramento de vulnerabilidades

O componente Monitoramento de Vulnerabilidades está desativado por padrão. É possível ativar o Monitoramento de Vulnerabilidades, se necessário.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

Para ativar ou desativar o Monitoramento de Vulnerabilidades na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Controle de Endpoints**.

   A seção **Controle de Endpoints** é exibida.
4. Clique com to botão direito para exibir o menu de contexto da linha com as informações sobre o componente Monitoramento de vulnerabilidades.

   Será aberto um menu para a seleção de ações.
5. Execute uma das seguintes ações:

   - Para ativar o Monitoramento de Vulnerabilidades, selecione **Iniciar**.

     O ícone de status do componente , exibido à esquerda na linha de **Monitoramento de Vulnerabilidades**, muda para o ícone .

- Para desativar o Monitoramento de Vulnerabilidades, selecione **Interromper**.

  O ícone de status do componente , exibido à esquerda na linha de **Monitoramento de Vulnerabilidades**, muda para o ícone .

Para ativar ou desativar o Monitoramento de Vulnerabilidades na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione **Monitoramento de Vulnerabilidades**.

   Na parte direita da janela, serão apresentadas as configurações do componente Monitoramento de Vulnerabilidades.

3. Na parte direita da janela, execute uma das seguintes operações:

   - Se desejar que o Kaspersky Endpoint Security execute a verificação de vulnerabilidades de aplicativos que estão sendo executados pelo computador do usuário ou que são iniciados pelo usuário, marque a caixa de seleção **Ativar Monitoramento de Vulnerabilidades**.

   - Se não desejar que o Kaspersky Endpoint Security execute a verificação de vulnerabilidades de aplicativos que estão sendo executados pelo computador do usuário ou que são iniciados pelo usuário, desmarque a caixa de seleção **Ativar Monitoramento de Vulnerabilidades**.

4. Para salvar as alterações, clique no botão **Salvar**.

Controle de Dispositivo

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado com o Microsoft Windows para estações de trabalho. Este componente estará indisponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado no Microsoft Windows para servidores de arquivos.

Esta seção contém informações sobre o Controle de Dispositivo e as instruções para definir as configurações do componente.

Sobre o Controle de Dispositivo

O Controle de Dispositivo assegura a proteção dos dados pessoais ao restringir o acesso do usuário a dispositivos instalados no computador ou conectados a este, incluindo:

- Dispositivos de armazenamento de dados (discos rígidos, unidades removíveis, unidades de fita, unidades de CD/DVD)
- Ferramentas de armazenamento de dados (modens, placas de rede externas)
- Dispositivos desenvolvidos para conversão de dados de impressão (impressoras)
- Barramentos de conexão (também referidos simplesmente como "barramentos"), referindo a interfaces para conexão de dispositivos a computadores (como USB, FireWire e Infravermelho)

O Controle de Dispositivo gerencia o acesso do usuário a dispositivos aplicando *regras de acesso a dispositivos* (também referidas como “regras de acesso”) e *regras de acesso a barramento de conexão* (também referidas como “regras de acesso a barramentos”).

Ativar e desativar o Controle de Dispositivo

Por padrão, o Controle de Dispositivo está ativado. É possível desativar o Controle de Dispositivo, se necessário.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

*Para ativar ou desativar o Controle de Dispositivo na guia **Proteção e Controle** da janela principal do aplicativo:*

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Controle de Endpoints**.

   A seção **Controle de Endpoints** é exibida.
4. Clique com o botão direito do mouse para abrir o menu de contexto da linha que contém as informações do componente Controle de Dispositivo.

Será aberto um menu para a seleção de ações.

5. Execute uma das seguintes ações:

   - Para ativar o Controle de Dispositivo, selecione **Iniciar** no menu.
   - Para desativar o Controle de Dispositivo, selecione **Interromper** no menu.

Para ativar ou desativar o Controle de Dispositivo na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.

   Na parte direita da janela, as configurações do componente Controle de Dispositivo serão apresentadas.
3. Execute uma das seguintes ações:

   - Se desejar ativar o Controle de Dispositivo, marque a caixa de seleção **Ativar o Controle de Dispositivo**.
   - Se desejar desativar o Controle de Dispositivo, desmarque a caixa de seleção **Ativar Controle de Dispositivo**.
4. Para salvar as alterações, clique no botão **Salvar**.

Sobre as regras de acesso a dispositivos e barramento de conexão

A regra de acesso de dispositivos é uma combinação de parâmetros que define as seguintes funções do Controle de Dispositivo:

- Permissão de usuários e/ou grupo de usuário selecionados para acessar tipos de dispositivos específicos durante certo período.

  Você pode selecionar um usuário e/ou grupo de usuário e criar um agendamento de acesso de dispositivos para eles.
- Definição de direitos para ler o conteúdo de dispositivos de memória.
- Definição de direitos para editar o conteúdo de dispositivos de memória.

Por padrão, regras de acesso são criadas para todos os tipos de dispositivos na classificação do componente de Controle de Dispositivo. Estas regras concedem a todos os usuários acesso total a dispositivos a qualquer momento, se o acesso aos barramento de conexão dos respectivos tipos de dispositivos for permitido.

A regra de acesso de barramento de conexão permite ou bloqueia o acesso ao barramento de conexão.

As regras que permitem o acesso aos barramentos são criadas por padrão para todos os barramento de conexão presentes na classificação do componente de Controle de Dispositivo.

Você não pode criar ou excluir regras de acesso de dispositivos ou regras de acesso de barramento de conexão; é possível somente editá-las.

Sobre os dispositivos confiáveis

Dispositivos confiáveis aqueles aos quais os usuários especificados têm acesso total a qualquer momento.

As seguintes operações de dispositivos confiáveis estão disponíveis:

- Adicionar o dispositivo à lista de dispositivos confiáveis.
- Alterar o usuário e/ou grupo de usuário com permissão de acesso ao dispositivo confiável.
- Excluir o dispositivo da lista de dispositivos confiáveis.

Ao adicionar o dispositivo à lista de dispositivos confiáveis e criar uma regra de acesso para este tipo de dispositivo, que bloqueia ou restringe o acesso, o Kaspersky Endpoint Security decide se concede acesso ao dispositivo estando este presente na lista de dispositivos confiáveis. A presença na lista de dispositivos confiáveis tem prioridade sobre a regra de acesso.

Decisões padrão de acesso a dispositivos

O Kaspersky Endpoint Security decide se permite ou não o acesso a um dispositivo quando o usuário o conecta ao computador.

Decisões padrão de acesso a dispositivos

Número	Condições iniciais	As etapas intermediárias a serem seguidas antes da decisão quanto ao acesso do dispositivo			Decisões de acesso a dispositivos
		Verificar se o dispositivo está incluído na lista de dispositivos confiáveis	Testar o acesso de dispositivo segundo a regra de acesso	Testar o acesso de barramento segundo a regra de acesso	
1	O dispositivo não se encontra na classificação de dispositivos do componente Controle de Dispositivo.	Não está incluído na lista de dispositivos confiáveis.	Nenhuma regra de acesso.	Não exige verificação.	Acesso permitido.
2	O dispositivo é confiável.	Incluído na lista de dispositivos confiáveis.	Não exige verificação.	Não exige verificação.	Acesso permitido.
3	O acesso ao dispositivo é permitido.	Não está incluído na lista de dispositivos confiáveis.	Acesso permitido.	Não exige verificação.	Acesso permitido.
4	O acesso ao dispositivo depende do barramento.	Não está incluído na lista de dispositivos confiáveis.	Acesso dependente do barramento.	Acesso permitido.	Acesso permitido.
5	O acesso ao dispositivo depende do barramento.	Não está incluído na lista de	Acesso dependente	Acesso bloqueado.	Acesso bloqueado.

		dispositivos confiáveis.	do barramento.		
6	O acesso ao dispositivo é permitido. Nenhuma regra de acesso de barramento encontrada.	Não está incluído na lista de dispositivos confiáveis.	Acesso permitido.	Nenhuma regra de acesso de barramento.	Acesso permitido.
7	O acesso ao dispositivo está bloqueado.	Não está incluído na lista de dispositivos confiáveis.	Acesso bloqueado.	Não exige verificação.	Acesso bloqueado.
8	Nenhuma regra de acesso de dispositivos ou regra de acesso de barramento foi encontrada.	Não está incluído na lista de dispositivos confiáveis.	Nenhuma regra de acesso.	Nenhuma regra de acesso de barramento.	Acesso permitido.
9	Nenhuma regra de acesso de dispositivos.	Não está incluído na lista de dispositivos confiáveis.	Nenhuma regra de acesso.	Acesso permitido.	Acesso permitido.
10	Nenhuma regra de acesso de dispositivos.	Não está incluído na lista de dispositivos confiáveis.	Nenhuma regra de acesso.	Acesso bloqueado.	Acesso bloqueado.

Você pode editar a regra de acesso de dispositivos quando conectar o dispositivo. Se o dispositivo está conectado, e tem permissão de acesso pela regra de acesso, isto não impede que você decida editar a regra de acesso e bloquear este posteriormente. Dessa forma, o Kaspersky Endpoint Security bloqueará o acesso na próxima vez que alguma operação com arquivos for solicitada pelo dispositivo, como visualizar a árvore de pastas, leitura, gravação. O dispositivo que não está no sistema de arquivos é bloqueado somente na próxima vez que for conectado.

Se um usuário do computador com Kaspersky Endpoint Security instalado precisar solicitar acesso a um dispositivo que o usuário acredita estar bloqueado por engano, envie ao usuário as instruções de acesso a solicitação.

Editar uma regra de acesso de dispositivos

Dependendo do tipo do dispositivo, você pode modificar várias configurações de acesso, como a lista de usuários que recebem acesso ao dispositivo, o agendamento de acesso, e acesso permitido/bloqueado.

Para editar uma regra de acesso de dispositivo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.

   Na parte direita da janela, as configurações do componente Controle de Dispositivo serão apresentadas.
3. Na parte direita da janela, selecione a guia **Tipos de dispositivos**.

   A guia **Tipos de dispositivos** contém as regras de acesso de todos os dispositivos classificados no componente Controle de Dispositivo.
4. Selecione a regra de acesso que deseja editar.

5. Clique no botão **Editar**. Este botão estará disponível somente para os tipos de dispositivos com um sistema de arquivos.

   A janela **Configurando regra de acesso de dispositivo** é aberta.

   Por padrão, uma regra de acesso de dispositivos concede a todos os usuários acesso total a todos os tipos de dispositivos especificados a qualquer momento. Na lista **Usuários e/ou grupos de usuários**, esta regra de acesso contém o grupo **Todos**. Na tabela **Direitos do grupo selecionado de usuários por agendamentos de acesso**, esta regra de acesso contém o **Agendamento padrão** para acesso a dispositivos, com direitos para executar todos os tipos de operações com os dispositivos.

6. Editar as configurações da regra acesso de dispositivos:

   a. Selecione um usuário e/ou grupo de usuários na lista **Usuários e/ou grupos de usuários**.

      Para editar a lista de **Usuários e/ou grupos de usuários**, utilize os botões **Adicionar**, **Editar** e **Remover**.

   b. Na tabela **Direitos do grupo selecionado de usuários por agendamentos de acesso**, configure o agendamento de acesso de dispositivos para o usuário e/ou grupo de usuários especificado. Para fazer isso, marque as caixas de seleção junto aos nomes dos agendamentos de acesso de dispositivos que deseja usar na regra de acesso de dispositivos a ser editada.

      Para editar a lista de agendamento de acesso a dispositivos, utilize os botões **Criar**, **Editar**, **Copiar** e **Remover** na tabela **Direitos do grupo selecionado de usuários por agendamentos de acesso**.

   c. Para cada agendamento do acesso a dispositivos usados na regra que é editada, especifique as operações que são permitidas ao trabalhar com dispositivos. Para fazer isso, na tabela **Direitos do grupo selecionado de usuários por agendamentos de acesso**, marque as caixas de seleção nas colunas com os nomes das operações relevantes.

   d. Clique em **OK**.

   Depois que você editou as configurações padrão de uma regra de acesso a dispositivo, a definição do acesso para o tipo de dispositivo na coluna **Acesso** na tabela, na guia **Tipos de dispositivos**, é modificada para o valor *Restringir por regras*.

7. Para salvar as alterações, clique no botão **Salvar**.

Adicionar ou excluir registros de eventos

O registro de evento está disponível somente para operações com arquivos em unidades removíveis.

Para ativar ou desativar o registro de evento:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.

   Na parte direita da janela, as configurações do componente Controle de Dispositivo serão apresentadas.

3. Na parte direita da janela, selecione a guia **Tipos de dispositivos**.

   A guia **Tipos de dispositivos** contém as regras de acesso de todos os dispositivos classificados no componente Controle de Dispositivo.

4. Selecionar **Unidades removíveis** na tabela de dispositivos.

O botão **Registro** fica disponível na parte superior da tabela.

5. Clique no botão **Registro**.

   Isto abre a janela **Configurações de registro**.

6. Execute uma das seguintes ações:

   - Se desejar ativar o registro da exclusão de arquivos e escrever operações em unidades removíveis, selecione a caixa **Ativar o registro**.

     O Kaspersky Endpoint Security salvará um evento no arquivo de registro e enviará uma mensagem ao Servidor de Administração do Kaspersky Security Center sempre que o usuário executar operações de escrita ou exclusão nos arquivos em unidades removíveis.

   - Caso contrário, desmarque a caixa **Ativar o registro**.

7. Especifique quais operações devem ser registradas. Para isso, execute uma das seguintes operações:

   - Se desejar que o Kaspersky Endpoint Security registre todos os eventos, marque a caixa de seleção **Salvar informações sobre todos os arquivos**.

   - Se desejar que o Kaspersky Endpoint Security só registre informações sobre arquivos de um formato específico, na seção **Filtrar em formatos de arquivo**, marque as caixas de seleção em frente dos formatos de arquivo relevantes.

8. Especifique quais as ações dos usuários do Kaspersky Endpoint Security devem ser registradas como eventos. Para fazer isso:

   a. Na seção **Usuários**, clique no botão **Selecionar**.

      A janela padrão **Selecionar Usuários ou Grupos**, no Microsoft Windows, abre.

   b. Especifique ou edite a lista de usuários e/ou os grupos dos usuários.

   Quando os usuários especificados na seção **Usuários** gravam em arquivos localizados em unidades removíveis ou excluem arquivos de unidades removíveis, o Kaspersky Endpoint Security salva as informações sobre tais operações no log de eventos e envia uma mensagem ao Servidor de Administração do Kaspersky Security Center.

9. Na janela **Configurações de registro**, clique em **OK**.

10. Para salvar as alterações, clique no botão **Salvar**.

Você pode exibir eventos associados com arquivos em unidades removíveis no Console de Administração do Kaspersky Security Center na área de trabalho do nó **Servidor de Administração** na guia **Eventos**. Para que os eventos sejam exibidos no registro de eventos do Kaspersky Endpoint Security local, você deve marcar a caixa de seleção **Operação de arquivo realizada** nas configurações de notificação para o componente Controle de Dispositivo.

Adicionar uma rede Wi-Fi à lista confiável

Você pode permitir que usuários conectem redes Wi-Fi que você considera segura, como uma rede Wi-Fi corporativa. Para fazer isso, você deve adicionar a rede à lista de redes Wi-Fi confiáveis. O Controle de Dispositivo bloqueará o acesso a todas as redes Wi-Fi, exceto aquelas especificadas na lista confiável.

Para adicionar uma rede Wi-Fi à lista confiável:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.

   Na parte direita da janela, as configurações do componente Controle de Dispositivo serão apresentadas.
3. Na parte direita da janela, selecione a guia **Tipos de dispositivos**.

   A guia **Tipos de dispositivos** contém as regras de acesso de todos os dispositivos classificados no componente Controle de Dispositivo.
4. Na coluna **Acesso** em frente do dispositivo **Wi-Fi**, clique com o botão direito para abrir o menu de contexto.
5. Selecione a opção **Bloquear com exceções**.
6. Na lista de dispositivos, selecione **Wi-Fi** e clique no botão **Editar**.

   É exibida a janela **Redes Wi-Fi confiáveis**.
7. Clique no botão **Adicionar**.

   É exbida a janela **Rede Wi-Fi confiável**.
8. Na janela **Rede Wi-Fi confiável**:

   - No campo **Nome de rede**, especifique o nome da rede Wi-Fi que você deseja adicionar à lista confiável.
   - Na lista suspensa **Tipo de autenticação**, selecione o tipo da autenticação usada ao conectar-se à rede Wi-Fi confiável.
   - Na lista suspensa **Tipo de criptografia**, selecione o tipo da criptografia usada para proteger o tráfego da rede Wi-Fi confiável.
   - No campo **Comentário**, é possível especificar qualquer informação sobre a rede Wi-Fi adicionada.

   Uma rede Wi-Fi será considerada confiável se as suas configurações coincidirem com todas as configurações especificadas na regra.
9. Na janela **Rede Wi-Fi confiável**, clique em **OK**.
10. Na janela **Redes Wi-Fi confiáveis**, clique em **OK**.

Editar uma regra de acesso de barramento de conexão

Para editar uma regra de acesso de barramento de conexão:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.

   Na parte direita da janela, as configurações do componente Controle de Dispositivo serão apresentadas.
3. Selecione a guia **Barramento de conexão**.

   A guia **Barramento de conexão** exibe as regras de acesso de todos os barramento de conexão que estão classificados no componente Controle de Dispositivo.

4. Selecione a regra de barramento de conexão que deseja editar.

5. Altere o valor do parâmetro de acesso:

   - Para permitir o acesso a um barramento de conexão, clique na coluna **Acesso** para abrir um menu de contexto e selecione **Permitir**.

   - Para bloquear o acesso a um barramento de conexão, clique na coluna **Acesso** para abrir um menu de contexto e selecione **Bloquear**.

6. Para salvar as alterações, clique no botão **Salvar**.

Ações com dispositivos confiáveis

Esta seção contém informações sobre ações com dispositivos confiáveis.

Adicionar um dispositivo à lista Confiável a partir da interface do aplicativo

Por padrão, quando um dispositivo é adicionado à lista de dispositivos confiáveis, o acesso a este é concedido a todos os usuários (ao grupo Todos os usuários).

Para adicionar um dispositivo à lista Confiável a partir da interface do aplicativo:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.

   Na parte direita da janela, as configurações do componente Controle de Dispositivo serão apresentadas.

3. À direita da janela, selecione a guia **Dispositivos confiáveis**.

4. Clique no botão **Selecionar**.

   A janela **Selecionar dispositivos confiáveis** é exibida.

5. Você pode marcar a caixa de seleção próxima ao nome do dispositivo que deseja adicionar à lista de dispositivos confiáveis.

   A lista apresentada na coluna **Dispositivos** depende do valor que é selecionado na lista suspensa **Exibir dispositivos conectados**.

6. Clique no botão **Selecionar**.

   A janela **Selecionar Usuários ou Grupos**, no Microsoft Windows, abre.

7. Na janela **Selecionar Usuários ou Grupos**, no Microsoft Windows, especifique os usuários e / ou grupos de usuários para os quais o Kaspersky Endpoint Security considera os dispositivos selecionados como confiáveis.

   Os nomes de usuários e / ou grupos de usuários especificados na janela **Selecionar usuários e/ou Grupos de usuários**, no Microsoft Windows, são exibidos no campo **Permitido a usuários e/ou grupos de usuários**.

8. Na janela **Selecionar dispositivos confiáveis**, clique em **OK**.

   Na tabela, na guia **Dispositivos confiáveis** da janela das configurações do componente **Controle de Dispositivo**, aparece uma linha exibindo os parâmetros do dispositivo confiável que foi adicionado.

9. Repita as etapas de número 4 a 7 para cada dispositivo que deseja adicionar à lista de dispositivos confiáveis para os usuários e/ou grupos de usuários especificados.

10. Para salvar as alterações, clique no botão **Salvar**.

Adicionar dispositivos à lista Confiável com base no modelo ou ID do dispositivo

Por padrão, quando um dispositivo é adicionado à lista de dispositivos confiáveis, o acesso a este é concedido a todos os usuários (ao grupo Todos os usuários).

Para adicionar dispositivos à lista Confiável com base no modelo ou ID do dispositivo:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual você deseja criar uma lista de dispositivos confiáveis.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.

   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.

7. À direita da janela, selecione a guia **Dispositivos confiáveis**.

8. Clique no botão **Adicionar**.

   O menu de contexto do botão é exibido.

9. No menu de contexto do botão **Adicionar**, execute uma das seguintes operações:

   - Selecione o botão **Dispositivos por ID** se desejar selecionar dispositivos com IDs exclusivos conhecidas para adicionar à lista de dispositivos confiáveis.

   - Selecione o item **Dispositivos por modelo** para adicionar à lista de dispositivos confiáveis cujas VID (ID do fornecedor) e PID (ID do produto) são conhecidas.

10. Na janela exibida, na lista suspensa **Tipo do dispositivo**, selecione o tipo de dispositivos a exibir na tabela embaixo.

11. Clique no botão **Atualizar**.

    A tabela exibe uma lista de dispositivos para os quais as IDs de dispositivo e/ou modelos são conhecidos e pertencem ao tipo selecionado na lista suspensa **Tipo do dispositivo**.

12. Selecione as caixas junto dos nomes de dispositivos que você deseja adicionar à lista de dispositivos confiáveis.

13. Clique no botão **Selecionar**.

    A janela **Selecionar Usuários ou Grupos**, no Microsoft Windows, abre.

14. Na janela **Selecionar Usuários ou Grupos**, no Microsoft Windows, especifique os usuários e / ou grupos de usuários para os quais o Kaspersky Endpoint Security considera os dispositivos selecionados como confiáveis.

    Os nomes de usuários e / ou grupos de usuários especificados na janela **Selecionar usuários e/ou Grupos de usuários**, no Microsoft Windows, são exibidos no campo **Permitido a usuários e/ou grupos de usuários**.

15. Clique em **OK**.

    As linhas aparecem com os parâmetros dos dispositivos confiáveis que foram adicionados aparecem na tabela da guia **Dispositivos confiáveis**.

16. Clique em **OK** ou em **Aplicar** para salvar as alterações.

Adicionar dispositivos à lista Confiável com base na máscara da ID do dispositivo

Por padrão, quando um dispositivo é adicionado à lista de dispositivos confiáveis, o acesso a este é concedido a todos os usuários (ao grupo Todos os usuários).

Os dispositivos podem ser adicionados à lista Confiável com base na máscara da sua ID somente no Console de Administração do Kaspersky Security Center.

Para adicionar dispositivos à lista Confiável com base na máscara da sua ID:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual você deseja criar uma lista de dispositivos confiáveis.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.
7. À direita da janela, selecione a guia **Dispositivos confiáveis**.
8. Clique no botão **Adicionar**.

   O menu de contexto do botão é exibido.

9. No menu de contexto do botão **Adicionar**, selecione o item **Dispositivos por máscara de ID**.

   A janela **Adicionar dispositivos confiáveis por máscara de ID**.

10. Na janela **Adicionar dispositivos confiáveis por máscara de ID**, insira a máscara para IDs de dispositivo no campo **Máscara**.

11. Clique no botão **Selecionar**.

    A janela **Selecionar Usuários ou Grupos**, no Microsoft Windows, abre.

12. Na janela **Selecionar usuários ou grupos** no Microsoft Windows, especifique usuários e/ou grupos de usuários cujos dispositivos o Kaspersky Endpoint Security reconhece como confiáveis com base nos modelos ou IDs correspondentes à máscara especificada.

    Os nomes de usuários e / ou grupos de usuários especificados na janela **Selecionar usuários e/ou Grupos de usuários**, no Microsoft Windows, são exibidos no campo **Permitido a usuários e/ou grupos de usuários**.

13. Clique em **OK**.

    Na tabela da guia **Dispositivos confiáveis** da janela de configurações do componente **Controle de Dispositivo**, aparece uma linha com as configurações da regra para adicionar dispositivos à lista de dispositivos confiáveis pela máscara de suas IDs.

14. Para salvar as alterações, clique no botão **Salvar**.

Configurar acesso do usuário a um dispositivo confiável

Por padrão, quando um dispositivo é adicionado à lista de dispositivos confiáveis, o acesso a este é concedido a todos os usuários (ao grupo Todos os usuários). Você pode configurar o acesso de usuários (ou grupo de usuários) a um dispositivo confiável.

Para configurar o acesso do usuário a um dispositivo confiável:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.

   Na parte direita da janela, as configurações do componente Controle de Dispositivo serão apresentadas.

3. À direita da janela, selecione a guia **Dispositivos confiáveis**.

4. Na lista de dispositivos confiáveis, selecione um dispositivo para o qual você deseja editar regras de acesso.

5. Clique no botão **Editar**.

   A janela **Configurar regra de acesso de dispositivo confiável** é aberta.

6. Clique no botão **Selecionar**.

   A janela **Selecionar Usuários ou Grupos**, no Microsoft Windows, abre.

7. Na janela **Selecionar Usuários ou Grupos**, no Microsoft Windows, especifique os usuários e / ou grupos de usuários para os quais o Kaspersky Endpoint Security considera os dispositivos selecionados como confiáveis.

8. Clique em **OK**.

   Os nomes de usuários e/ou grupos de usuários especificados na janela **Selecionar usuários e/ou grupos de usuários**, no Microsoft Windows, são exibidos no campo **Permitido a usuários e/ou grupos de usuários** da janela **Configurar regra de acesso de dispositivo confiável**.

9. Clique em **OK**.

10. Para salvar as alterações, clique no botão **Salvar**.

Remover um dispositivo da lista de dispositivos confiáveis

Para remover um dispositivo da lista de dispositivos confiáveis:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.
   Na parte direita da janela, as configurações do componente Controle de Dispositivo serão apresentadas.
3. À direita da janela, selecione a guia **Dispositivos confiáveis**.
4. Selecione o dispositivo que deseja remover da lista de dispositivos confiáveis.
5. Clique no botão **Remover**.
6. Para salvar as alterações, clique no botão **Salvar**.

A decisão quanto ao acesso a dispositivo que foi removido da lista de dispositivos confiáveis é feita pelo Kaspersky Endpoint Security segundo as regras de acesso de dispositivos e as de acesso de barramento de conexão.

Editar os modelos de mensagens do Controle de Dispositivo

Quando o usuário tenta obter acesso a um dispositivo bloqueado, o Kaspersky Endpoint Security exibe uma mensagem informando que o acesso ao dispositivo está bloqueado ou que a execução com o conteúdo do dispositivo não é permitida. Se o usuário acredita que o acesso ao dispositivo foi erroneamente bloqueado ou que uma operação com o conteúdo do dispositivo foi proibida por engano, o usuário pode enviar uma mensagem ao administrador de rede corporativa local clicando no link na mensagem exibida sobre a ação bloqueada.

Estão disponíveis modelos para mensagens sobre o acesso bloqueado a dispositivos ou operações proibidas com conteúdo do dispositivo, e para a mensagem enviada ao administrador. Você pode modificar os modelos de mensagem.

Para editar os modelos das mensagens do Controle de Dispositivo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Controle de Endpoints**, selecione a subseção **Controle de Dispositivo**.
   Na parte direita da janela, as configurações do componente Controle de Dispositivo serão apresentadas.
3. Na parte direita da janela, clique no botão **Modelos**.
   A janela **Modelos de mensagem** é exibida.
4. Execute uma das seguintes ações:
   - Para alterar o modelo da mensagem de bloqueio do acesso ao dispositivo ou de não permissão da operação com o conteúdo do dispositivo, selecione a guia **Bloqueio**.

- Para modificar o modelo da mensagem que é enviada ao administrador da rede local, selecione a guia **Mensagem para o administrador**.

5. Editar o modelo de mensagem. Você também pode usar os seguintes botões: **Variável**, **Padrão** e **Link** (este botão está disponível apenas na guia **Bloqueio**).

6. Clique em **OK**.

7. Para salvar as alterações, clique no botão **Salvar**.

Obter acesso a um dispositivo bloqueado

Estas instruções são destinadas para usuários de computadores de cliente com Kaspersky Endpoint Security instalado.

O recurso do Kaspersky Endpoint Security que permite o acesso temporário ao dispositivo está disponível somente quando o Kaspersky Endpoint Security é executado segundo a política do Kaspersky Security Center e este recurso está ativo nas configurações da política. (Consulte o *Guia do Administrador do Kaspersky Security Center*).

Para solicitar acesso a um dispositivo bloqueado usando a janela de configurações do componente Controle de Dispositivo:

1. Na janela do aplicativo principal, selecione a guia **Proteção e Controle**.

2. Clique na seção **Controle de Endpoints**.

   A seção **Controle de Endpoints** é exibida.

3. Clique com o botão direito do mouse para abrir o menu de contexto da linha que contém as informações do componente Controle de Dispositivo.

   Será aberto um menu para a seleção de ações.

4. Clique no botão **Acesso a dispositivo**.

   A janela **Solicitar acesso ao dispositivo** é exibida.

5. Selecione o dispositivo que deseja acessar na lista de dispositivos conectados.

6. Clique no botão **Gerar arquivo de solicitação de acesso**.

   É exibida a janela **Criando arquivo de solicitação de acesso**.

7. No campo **Duração do acesso**, especifique o intervalo de tempo em que você deseja ter acesso ao dispositivo.

8. Clique no botão **Salvar**.

   É exibida a janela padrão do Microsoft Windows, **Salvar o arquivo de solicitação de acesso**.

9. Na janela do Microsoft Windows **Salvar o arquivo de solicitação de acesso**, selecione a pasta em que deseja salvar o arquivo de solicitação de acesso no dispositivo e clique no botão **Salvar**.

10. Envie o arquivo de solicitação de acesso ao dispositivo ao administrador da rede.

11. Receba o arquivo com a chave de acesso do dispositivo do administrador da rede.

12. Na janela **Solicitar acesso ao dispositivo**, clique no botão **Ativar chave de acesso**.

    A janela padrão do Microsoft Windows **Abrir chave de acesso** é exibida.

13. Na janela do Microsoft Windows **Abrir chave de acesso**, selecione o arquivo com a chave de acesso do dispositivo recebido do administrador da rede e clique em **Abrir**.

    A janela **Ativando a chave de acesso do dispositivo** abre e exibe informações sobre o acesso concedido.

14. Na janela **Ativando a chave de acesso do dispositivo**, clique em **OK**.

Para solicitar acesso a um dispositivo bloqueado clicando no link da mensagem de informação sobre o bloqueio do dispositivo:

1. Na janela com a mensagem de informação sobre o bloqueio do dispositivo ou do barramento de conexão, clique no link **Solicitar acesso**.

   É exibida a janela **Criando arquivo de solicitação de acesso**.

2. No campo **Duração do acesso**, especifique o intervalo de tempo em que você deseja ter acesso ao dispositivo.

3. Clique no botão **Salvar**.

   É exibida a janela padrão do Microsoft Windows, **Salvar o arquivo de solicitação de acesso**.

4. Na janela do Microsoft Windows **Salvar o arquivo de solicitação de acesso**, selecione a pasta em que deseja salvar o arquivo de solicitação de acesso no dispositivo e clique no botão **Salvar**.

5. Envie o arquivo de solicitação de acesso ao dispositivo ao administrador da rede.

6. Receba o arquivo com a chave de acesso do dispositivo do administrador da rede.

7. Na janela **Solicitar acesso ao dispositivo**, clique no botão **Ativar chave de acesso**.

   A janela padrão do Microsoft Windows **Abrir chave de acesso** é exibida.

8. Na janela do Microsoft Windows **Abrir chave de acesso**, selecione o arquivo com a chave de acesso do dispositivo recebido do administrador da rede e clique em **Abrir**.

   A janela **Ativando a chave de acesso do dispositivo** abre e exibe informações sobre o acesso concedido.

9. Na janela **Ativando a chave de acesso do dispositivo**, clique em **OK**.

O período de tempo de acesso permitido ao dispositivo pode ser diferente daquele que solicita. O acesso ao dispositivo é concedido para o período de tempo especificado pelo administrador da rede ao gerar a chave de acesso do dispositivo.

Criar uma chave para acessar um dispositivo bloqueado usando o Kaspersky Security Center

Para conceder ao usuário acesso temporário a um dispositivo bloqueado, é necessário ter uma chave de acesso. Você pode criar uma chave de acesso utilizando o Kaspersky Security Center.

Para criar uma chave de acesso para um dispositivo bloqueado:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** da árvore Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertence o computador cliente desejado.

3. No espaço de trabalho, selecione a guia **Dispositivos**.

4. Na lista de computadores clientes, selecione o computador do usuário que precisa de permissão para acessar o dispositivo bloqueado temporariamente.

5. No menu de contexto do computador, selecione **Conceder acesso a dispositivos e dados em modo off-line**.

   A janela **Conceder acesso a dispositivos e dados em modo off-line** é exibida.

6. Selecione a guia **Controle de Dispositivo**.

7. Na guia **Controle de Dispositivo**, clique no botão **Procurar**.

   A janela do Microsoft Windows **Selecionar o arquivo de solicitação de acesso** é exibida.

8. Na janela **Selecionar o arquivo de solicitação de acesso**, selecione o arquivo de solicitação de acesso que você recebeu do usuário e clique no botão **Abrir**.

   O **Controle de Dispositivo** exibe detalhes do dispositivo bloqueado ao qual o usuário solicitou acesso.

9. Especifique o valor para a configuração **Duração do acesso**.

   Esta configuração define a duração do acesso que você concede ao usuário para acessar o dispositivo bloqueado. O valor padrão é igual ao especificado pelo usuário ao criar o arquivo de solicitação de acesso.

10. Especifique o valor para a configuração **Período de ativação**.

    Essa configuração define o período durante o qual o usuário pode ativar o acesso para o dispositivo bloqueado com uma chave de acesso fornecida.

11. Clique no botão **Salvar**.

    Isso abre a janela **Salvar chave de acesso** do Microsoft Windows.

12. Selecione a pasta de destino em que deseja salvar o arquivo com a chave de acesso do dispositivo bloqueado.

13. Clique no botão **Salvar**.

Controle da Web

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado com o Microsoft Windows para estações de trabalho. Este componente estará indisponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado no Microsoft Windows para servidores de arquivos.

Esta seção contém informações sobre o Controle da Web e as instruções para definir as configurações do componente.

Sobre o Controle da Web

O Controle da Web permite controlar as ações de usuário da rede local restringindo ou bloqueando o acesso de recursos da Web.

O recurso da Web refere-se a uma página da Web ou a páginas diversas, ou a um site ou a sites diversos reunidos por características comuns.

O Controle da Web oferece as seguintes opções:

- Economizar tráfego.

  O tráfego é controlado pela restrição ou bloqueio de downloads de arquivos de multimídia, pela restrição ou bloqueio de acesso de recursos da Web que não estão relacionados às atividades de trabalho do usuário.

- Delimitação de acesso de recursos da Web por categorias de conteúdo.

  Para economizar tráfego e reduzir possíveis prejuízos devido ao desperdício de tempo no computador pelo funcionário, você pode restringir ou bloquear o acesso a certas categorias de recursos da Internet (por exemplo, bloquear o acesso a recursos da Web pertencentes à categoria "Mídia de comunicação da Internet").

- Controle centralizado do acesso a recursos da Web.

  O Kaspersky Security Center disponibiliza configurações de acesso a recursos da Web individuais e de grupo.

Todas as restrições e os blocos que são aplicados ao acesso a recursos da Web são implementados como regras de acesso a recurso de Web.

Ativar e desativar o Controle da Web

Por padrão, o Controle da Web está ativo. É possível desativar o Controle da Web, se necessário.

Existem duas maneiras para ativar e desativar o componente:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

*Para ativar ou desativar o Controle da Web na guia **Proteção e Controle** da janela principal do aplicativo:*

1. Abra a janela principal do aplicativo.

2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Controle de Endpoints**.

   A seção **Controle de Endpoints** é exibida.
4. Clique com o botão direito para abrir o menu de contexto da linha que contém informações do componente Controle da Web.

   Será aberto um menu para a seleção de ações.
5. Execute uma das seguintes ações:

   - Para ativar o Controle da Web, selecione **Iniciar** no menu.
   - Para desativar o Controle da Web, selecione **Interromper** no menu.

Para ativar ou desativar o Controle da Web na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Controle de Endpoints**, selecione **Controle da Web**.

   À direita da janela, as configurações do componente de Controle da Web serão apresentadas.
3. Execute uma das seguintes ações:

   - Se desejar ativar o Controle da Web, marque a caixa de seleção **Ativar Controle da Web**.
   - Se desejar desativar o Controle da Web, desmarque a caixa de seleção **Ativar Controle da Web**.

   Se o Controle da Web for desativado, o Kaspersky Endpoint Security não controlará o acesso a recursos da Web.
4. Para salvar as alterações, clique no botão **Salvar**.

Categorias de conteúdo de recurso da Web

As categorias de conteúdo dos recursos da Web (doravante também referidas como "categorias") listadas embaixo foram selecionadas para descrever da forma mais completa os blocos de dados alojados pelos recursos da Web, tendo em conta sua especificidade funcional e temática. A ordem pela qual as categorias da Web são exibidas nessa lista não reflete a importância relativa ou a prevalência dessas categorias na Internet. Os nomes das categorias são provisórios e usados apenas para o propósito de produtos e sites da Kaspersky. Os nomes não refletem necessariamente o significado implicado por lei. Um recurso da Web pode pertencer a várias categorias simultaneamente.

Conteúdo para adultos

Essa categoria inclui os seguintes tipos de recursos da Web:

- Recursos da Web que contêm qualquer foto ou vídeo exibindo os órgãos genitais de humanos ou criaturas humanóides, atos de relação sexual ou autoestímulo realizados por seres humanos ou criaturas humanóides.
- Recursos da Web que contêm materiais de texto, incluindo materiais literários ou artísticos que descrevam os órgãos genitais de humanos ou criaturas humanóides, atos de relação sexual ou autoestímulo realizados por

seres humanos ou criaturas humanóides.

- Recursos da Web dedicados ao debate dos aspetos sexuais das relações entre seres humanos.

  Sobrepõe-se com a categoria "Mídia em comunicações na Internet".

- Recursos da Web que contêm materiais eróticos, trabalhos que forneçam um retrato realista do comportamento sexual de humanos ou obras de arte concebidas para estimular a excitação sexual.
- Recursos da Web de mídia oficial e comunidades on-line com uma elevada audiência estabelecida e que contenham uma seção especial e/ou artigos individuais dedicados aos aspetos sexuais das relações entre seres humanos.
- Recursos da Web dedicados a perversões sexuais.
- Recursos da Web que publicitam e vendem itens para utilização em atos sexuais e no estímulo da excitação sexual, serviços sexuais e encontros íntimos, incluindo serviços fornecidos por canais de bate-papo ou de vídeo erótico on-line, “sexo por telefone”, “mensagens de texto de cariz sexual” (“sexo virtual”).
- Recursos da Web com os seguintes conteúdos:
  - Artigos e blogs que cobrem educação sexual com temas científicos e populares.
  - Enciclopédias médicas, especificamente seções sobre reprodução sexual.
  - Recursos de instituições médicas, especificamente seções que cobrem tratamento de órgãos sexuais.

Software, áudio, vídeo

Essa categoria inclui as seguintes subcategorias que você pode selecionar individualmente:

- **Áudio e vídeo**.

  Essa subcategoria inclui recursos da Web que distribuem materiais de áudio e vídeo: filmes, gravações de transmissões esportivas, gravações de concertos, músicas, clipes de filmes, vídeos, gravações em vídeo e áudio de tutoriais, etc.

- **Torrents**.

  Esta subcategoria inclui sites de controladores do torrents destinados a compartilhar arquivos de tamanho ilimitado.

- **Compartilhamento de Arquivos**.

  Esta subcategoria inclui sites de compartilhamento de arquivo independentes da posição física de arquivos que são distribuídos.

Álcool, tabaco, drogas

Essa categoria inclui recursos da Web cujo conteúdo está direta ou indiretamente relacionado com produtos alcoólicos ou que contêm álcool, produtos de tabaco e substâncias narcóticas, psicotrópicas e/ou intoxicantes.

- Recursos da Web que anunciam e vendem essas substâncias e equipamento para o seu consumo.

Sobrepõe-se com a categoria “Comércio eletrônico”.

- Recursos da Web com instruções sobre como consumir ou produzir narcóticos, substâncias psicotrópicas e/ou intoxicantes.

Essa categoria inclui recursos da Web que referenciam tópicos científicos e médicos.

Violência

Essa categoria inclui recursos da Web que contêm fotografias, vídeos ou materiais de texto que descrevem atos de violência física ou psicológica direcionados a seres humanos ou tratamento cruel de animais.

- Recursos da Web que descrevem ou exibem cenas de execuções, tortura ou abuso, bem como as ferramentas designadas para essas práticas.

  Sobrepõe-se com a categoria "Armas, explosivos, pirotecnia".

- Recursos da Web que descrevem ou exibem cenas de morte, espancamento ou estupro, cenas em que humanos ou animais ou criaturas imaginárias são abusados ou humilhados.
- Recursos da Web com informações que incitam a atos que colocam em perigo a integridade e/ou a vida, incluindo a automutilação ou o suicídio.
- Recursos da Web com informações que justifica ou comprova a admissibilidade da violência e/ou crueldade, ou que incitam a atos violentos contra humanos ou animais.
- Recursos da Web com retratos ou descrições particularmente realistas de vítimas e as atrocidades da guerra, de conflitos armados e sublevações militares, acidentes, catástrofes, desastres naturais, cataclismos industriais ou sociais ou sofrimento humano.
- Jogos de computador de navegador com cenas de violência e crueldade, incluindo os chamados "jogos de tiros", "luta", "slashers", etc.

  Sobrepõe-se com a categoria "Jogos de computador".

Armas, explosivos, pirotecnia

Essa categoria inclui os recursos da Web com informações sobre armas, explosivos e produtos pirotécnicos:

- Sites de fabricantes e lojas de armas, explosivos e produtos pirotécnicos.

  Sobrepõe-se com a categoria “Comércio eletrônico”.

- Recursos da Web dedicados ao fabrico e uso de armas, explosivos e produtos pirotécnicos.

- Recursos da Web que contêm materiais de análise, históricos, de fabrico e conteúdo enciclopédico sobre armas, explosivos e produtos pirotécnicos.

O termo "armas" significa a ferramenta, os itens e as formas concebidas para causar danos à integridade ou à vida de humanos e animais e/ou danificar equipamento e estruturas.

Obscenidades

Essa categoria inclui recursos da Web onde foi detectada linguagem obscena.

Sobrepõe-se com a categoria "Conteúdo para adultos".

Essa categoria inclui também recursos da Web com materiais linguísticos e filológicos que contêm obscenidade como objeto de estudo.

Jogos, loterias, apostas

Essa categoria inclui os recursos da Web que oferecem aos usuários a participação financeira em jogos, mesmo que essa participação financeira não seja uma condição obrigatória para acessar o site. Essa categoria inclui os recursos da Web que oferecem:

- Jogos nos quais os participantes devem fazer contributos monetários.

  Sobrepõe-se com a categoria "Jogos de computador".

- Apostas que envolvem dinheiro real.
- Loterias que envolvem a compra de bilhetes ou números de loteria.
- Informações que podem causar o desejo de participar de jogos, apostas e loterias.

Sobrepõe-se com a categoria “Comércio eletrônico”.

Essa categoria inclui jogos que oferecem participação gratuita como um modo separado, bem com recursos da Web que publicitam ativamente outros recursos da Web que se enquadram nessa categoria.

Comunicações de rede

Essa categoria inclui recursos da Web que permitem que os usuários (registrados ou não) enviem mensagens pessoais a outros usuários dos recursos da Web relevantes ou outros serviços on-line e/ou que adicionem conteúdo (quer aberto ao público ou com acesso restrito) aos recursos da Web relevantes de acordo com determinados termos. Você pode selecionar individualmente as seguintes subcategorias:

- **Bate-papo e fóruns**.

Essa subcategoria inclui recursos de Web destinados a discussão pública de vários tópicos usando aplicativos da Web especiais, bem como recursos da Web projetados para distribuir ou suportar aplicativos de mensagens instantâneas que ativam a comunicação em tempo real.

- **Blogs**.

  Essa subcategoria inclui plataformas de blog, que são sites que fornecem serviços pagos ou gratuitos para criar e manter blogs.

- **Redes sociais**.

  Essa subcategoria inclui sites concebidos para criar, exibir e gerenciar contatos entre pessoas, organizações e governos, os quais requerem um registro de uma conta de usuário como a condição para participação.

- **Sites de encontros**.

  Essa subcategoria inclui recursos da Web que servem de várias redes sociais que provêem serviços pagos ou gratuitos.

  Sobrepõe-se com as categorias "Conteúdo para adultos" e "Comércio eletrônico".

- **E-mail baseado na Web**.

  Essa subcategoria inclui exclusivamente páginas de login de um serviço de e-mail e páginas de caixa de correio com e-mails e dados associados (como os contatos pessoais). Essa categoria não inclui outras páginas da Web de um provedor de serviços na Internet que também ofereça serviço de e-mail.

Comércio eletrônico, bancos e sistemas de pagamento

Essa categoria inclui os recursos da Web concebidos para quaisquer transações on-line em fundos monetários não em numerário usando aplicativos da Web especiais. Você pode selecionar individualmente as seguintes subcategorias:

- **Lojas e leilões**.

  Essa subcategoria inclui lojas on-line e leilões on-line que vendem bens, trabalho ou serviços a indivíduos e/ou outras entidades, incluindo sites de lojas que conduzem vendas exclusivamente on-line e perfis on-line de lojas físicas que aceitam pagamento on-line.

- **Bancos**.

  Essa subcategoria inclui páginas da Web especializadas de bancos com funcionalidade bancária on-line, incluindo transferências eletrônicas entre contas bancárias, depósitos bancários, câmbio de moeda, pagamento de serviços de terceiros, etc.

- **Sistemas de pagamento**.

  Essa subcategoria inclui páginas da Web de sistemas de e-money que fornecem acesso à conta pessoal do usuário.

Em termos técnicos, o pagamento pode ser efetuado usando cartões bancários de qualquer tipo (plástico ou virtual, débito ou crédito, local ou internacional) e e-money. Recursos da Web podem ser incluídos nessa categoria independentemente de terem aspetos técnicos como a transmissão de dados através de protocolo SSL, o uso de autenticação 3D Secure, etc.

Pesquisa de emprego

Essa categoria inclui recursos da Web concebidos para unir empregadores e indivíduos que procuram emprego:

- Sites de agências de recrutamento (agências de emprego e/ou agência de caça de talentos).
- Sites de empregadores com descrições de vagas e suas vantagens.
- Portais independentes com ofertas de emprego de empregadores e agências de recrutamento.
- Redes sociais profissionais que, entre outras coisas, tornam possível publicar ou encontrar informações sobre especialistas que não estão ativamente à procura de um emprego.

> Sobrepõe-se com a categoria "Mídia em comunicações na Internet".

Sistemas de acesso anônimos

Essa categoria inclui recursos da Web que atuam como intermediário no download de conteúdo ou outros recursos da Web usando aplicativos da Web especiais para:

- Contornar as restrições impostas por um administrador de LAN no acesso a endereços da Web ou endereços IP;
- Acessar anonimamente recursos da Web, incluindo recursos da Web que especificamente rejeitam pedidos HTTP de determinados endereços IP ou seus grupos (por exemplo, endereços IP agrupados por país de origem).

Essa categoria inclui os recursos da Web concebidos exclusivamente para os efeitos descritos acima ("criadores de anonimato") e recursos da Web com funcionalidade técnica semelhante.

Jogos de computador

Essa categoria inclui recursos da Web dedicados a jogos de vários tipos:

- Sites de desenvolvedores de jogos de computador.
- Recursos da Web dedicados ao debate de jogos de computador.

> Sobrepõe-se com a categoria "Mídia em comunicações na Internet".

- Recursos da Web que fornecem a funcionalidade técnica para participação on-line em jogos, com outros participantes ou individualmente, com instalação local de aplicativos ou sem essa instalação (“jogos de navegador”).
- Recursos da Web concebidos para anunciar, distribuir e suportar software de jogo.

> Sobrepõe-se com a categoria “Comércio eletrônico”.

Religiões, associações religiosas

Essa categoria inclui recursos da Web com materiais sobre movimentos públicos, associações e organizações com uma ideologia religiosa e/ou culto em quaisquer manifestações.

- Sites de organizações religiosas oficiais em diferentes níveis, desde religiões internacionais até comunidades religiosas locais.
- Sites de associações religiosas não registradas e sociedades que surgiram através de uma separação de uma associação ou comunidade religiosa dominante.
- Sites de associações religiosas e comunidades que emergiram de forma independente dos movimentos religiosos tradicionais, incluindo a iniciativa de um fundador específico.
- Sites de organizações interconfessionais que procuram a cooperação entre representantes de diferentes religiões tradicionais.
- Recursos da Web com materiais acadêmicos, históricos e enciclopédicos sobre o tópico da religião.
- Recursos da Web com retratos detalhados ou descrições de devoção como parte de cultos religiosos, incluindo ritos e rituais que envolvem a adoração de deuses, seres e/ou itens que se acredita terem poderes sobrenaturais.

Mídia de notícias

Essa categoria inclui recursos da Web com conteúdo de notícias público criado pelos mídia ou publicações on-line que permitem que os usuários adicionem seus próprios relatórios de notícias:

- Sites de mídia oficial.
- Sites que oferecem serviços de informação com a atribuição de fontes oficiais de informação.
- Sites que oferecem serviços de agregação, de coletas de informação de notícias de várias fontes oficiais e não oficiais.
- Sites onde o conteúdo de notícias é criado pelos próprios usuários (“sites de notícias sociais”).

> Sobrepõe-se com a categoria "Mídia em comunicações na Internet".

Banners

Essa categoria inclui os recursos da Web com banners. As informações de anúncios em banners podem distrair os usuários de suas atividades, ao passo que os downloads de banners aumentam a quantidade de tráfego de entrada.

Sobre as regras de acesso de recurso da Web

A regra de acesso de recurso da Web é um conjunto de filtros e ações que o Kaspersky Endpoint Security executa quando o usuário visita os recursos da Web descritos na regra durante o período indicado no agendamento da regra. Os filtros permitem especificar de forma precisa um grupo de recursos da Web cujo acesso é controlado pelo componente de Controle da Web.

Os seguintes filtros estão disponíveis:

- **Filtro por conteúdo**. O Controle da Web categoriza recursos da Web por conteúdo e tipo de dados. Você pode controlar o acesso de usuários a recursos da Web com certas categorias de conteúdo e tipos de dados. Quando usuários visitam recursos da Web que pertencem à categoria de conteúdo selecionada e/ou de tipo de dados, o Kaspersky Endpoint Security executa a ação especificada na regra.

- **Filtro por endereços de recurso da Web**. Você pode controlar o acesso do usuário a todos os endereços de recurso da Web ou a endereços de recurso da Web individuais e a endereços de /ou grupos de endereços de recurso da Web.

  Ao especificar o filtro por conteúdo e por endereços de recurso da Web, e os endereços de recurso da Web e/ou grupos de endereços de recurso da Web especificados pertencem às categorias de conteúdo ou tipo de dados selecionadas, o Kaspersky Endpoint Security não controla o acesso de todos os recursos da Web nas categorias de conteúdo e/ou tipos de dados selecionadas. Em vez disso, o aplicativo controla o acesso somente dos endereços de recurso da Web e/ou grupos de endereços de recurso da Web especificados.

- **Filtrar por nomes de usuários e grupo de usuários**. Você pode especificar os nomes de usuários e / ou grupos de usuários com acesso a recursos da Web controlados segundo a regra.

- **Agendamento da regra**. É possível especificar a regra de agendamento. O agendamento da regra determina o período de tempo durante o qual o Kaspersky Endpoint Security monitora o acesso de recursos da Web abrangidos pela regra.

Após o Kaspersky Endpoint Security ser instalado, a lista de regras do componente de Controle da Web não fica em branco. São predefinidas duas regras:

- A regra das Tabelas Cenário e Estilo, que concede acesso a todos os usuários a qualquer momento a recursos da Web cujos endereços contêm nomes de arquivos com as extensões css, js, ou vbs. Por exemplo:http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- A "regra Padrão", que concede a todos os usuários acesso a recursos da Web a qualquer momento.

Ações com regras de acesso de recurso da Web

Você pode executar as seguintes ações com regras de acesso de recurso da Web:

- Adicionar nova regra

- Editar regra

- Atribuir prioridade à regra

  A prioridade de uma regra é definida pela posição da linha que contém uma breve descrição desta regra dentro da tabela de regras de acesso na janela de configurações do componente de Controle da Web. Isto significa que uma regra com prioridade mais alta na tabela de regras de acesso tem prioridade sobre aquela localizada abaixo dela.

  Se o recurso da Web que o usuário tenta acessar corresponde aos parâmetros de várias regras, o Kaspersky Endpoint Security executa uma ação segundo a regra com a prioridade mais alta.

- Testar regra.

  Você pode verificar a consistência das regras usando a função de diagnóstico das regras.

- Ativar ou desativar regra.

  A regra de acesso de recurso da Web pode ser ativada (status de operação: *Ativa*) ou desativada (status de operação: *Desativada*). Por padrão, após uma regra ser criada, ela estará ativa (status de operação: *Ativa)*. Você pode desativar regra.

- Excluir regra

Adicionar e editar a regra de acesso de recurso da Web

Para adicionar ou editar a regra de acesso de recurso da Web:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Controle de Endpoints**, selecione **Controle da Web**.
   À direita da janela, as configurações do componente de Controle da Web serão apresentadas.
3. Execute uma das seguintes ações:
   - Para adicionar uma regra, clique no botão **Adicionar**.
   - Se desejar editar uma regra, selecione a regra na tabela e clique no botão **Editar**.

   A janela **Regra de acesso a recursos da Web** é exibida.
4. Especifique ou edite as configurações da regra. Para fazer isso:
   a. No campo **Nome**, insira ou edite o nome da regra.
   b. Na lista suspensa **Filtrar conteúdo**, selecione a opção desejada:
      - **Qualquer conteúdo**.
      - **Por categorias de conteúdo**.
      - **Por tipos de dados**.
      - **Por categorias de conteúdo e tipos de dados**.
   c. Se uma opção diferente de **Qualquer conteúdo** for selecionada, serão abertas seções para selecionar categorias de conteúdo e/ou tipos de dados. Marque as caixas de seleção junto aos nomes das categorias de conteúdo necessárias e/ou de tipo de dados.
      Ao marcar as caixas de seleção junto aos nomes de uma categoria de conteúdo e/ou tipo de dados, o Kaspersky Endpoint Security aplica a regra para controlar o acesso a recursos da Web que pertencem às categorias de conteúdo e/ou tipos de dados selecionados.
   d. Na lista suspensa **Aplicar aos endereços**, selecione a opção desejada:
      - **Para todos os endereços**.
      - **Para endereços individuais**.
   e. Se selecionar a opção **Para endereços individuais**, é exibida uma seção para você criar uma lista de recursos da Web. Você pode adicionar ou editar os endereços dos recursos da Web por meio dos botões **Adicionar**, **Editar** e **Excluir**.
   f. Marque a caixa de seleção **Especificar usuários e/ou grupos**.
   g. Clique no botão **Selecionar**.

A janela **Selecionar Usuários ou Grupos**, no Microsoft Windows, abre.

h. Especifique ou edite a lista de usuários e/ou grupos de usuários cujo acesso aos recursos da Web descritos pela regra será permitido ou bloqueado.

i. Na lista suspensa **Ação**, selecione a opção desejada:

- **Permitir** Se este valor for selecionado, o Kaspersky Endpoint Security permitirá o acesso aos recursos da Web que correspondem às configurações da regra.
- **Bloquear** Se este valor for selecionado, o Kaspersky Endpoint Security bloqueará o acesso aos recursos da Web que correspondem às configurações da regra.
- **Avisar**. Se este valor for selecionado, quando o usuário tenta acessar um recurso da Web que corresponde à regra, o Kaspersky Endpoint Security exibirá uma mensagem de aviso informando que o recurso é indesejado. O usuário consegue obter o acesso ao recurso da Web desejado ao usar os links da mensagem de aviso.

j. Na lista suspensa **Agendamento da regra**, selecione o nome do agendamento desejado ou crie um novo com base no agendamento da regra selecionada. Para fazer isso:

1. Ao lado da lista suspensa **Agendamento da regra**, clique no botão **Configurações**.

   A janela **Agendamento da regra** é exibida.

2. Para adicionar ao agendamento da regra um período durante o qual a regra não é aplicada, na tabela que exibe o agendamento da regra, clique nas células da tabela que correspondem à hora e ao dia da semana desejados.

   A célula torna-se cinza.

3. Para substituir um período durante o qual a regra é aplicada por um período surante o qual a regra não é aplicada, clique nas células com fundo cinza na tabela que correspondem à hora e ao dia da semana desejados.

   A célula torna-se verde.

4. Clique no botão **Salvar como**.

   A janela **Nome do agendamento da regra** é exibida.

5. Digite o nome do agendamento da regra ou use o nome padrão que é sugerido.

6. Clique em **OK**.

5. Na janela **Regra de acesso a recursos da Web**, clique em **OK**.

6. Para salvar as alterações, clique no botão **Salvar**.

Atribuir prioridades às regras de acesso de recurso da Web

Você pode atribuir prioridades a cada regra na lista de regras, ordenando-as de forma determinada.

Para atribuir a prioridade de uma regra de acesso de recurso da Web:

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Controle de Endpoints**, selecione **Controle da Web**.

   À direita da janela, as configurações do componente de Controle da Web serão apresentadas.

3. À direita da janela, selecione a regra cuja prioridade deseja editar.

4. Use os botões **Mover para baixo** e **Mover para baixo** para mover a regra para o local pretendido na lista de regras.

5. Repita as etapas 3 e 4 para as regras cuja prioridade deseja editar.

6. Para salvar as alterações, clique no botão **Salvar**.

Testar as regras de acesso de recurso da Web

Para verificar a consistência de regras do Controle da Web, é possível testá-las. Para fazer isso, o componente Controle da Web inclui uma função de diagnóstico das regras.

Para testar as regras de acesso a recursos da Web:

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Controle de Endpoints**, selecione **Controle da Web**.

   À direita da janela, as configurações do componente de Controle da Web serão apresentadas.

3. Na parte direita da janela, clique no botão **Diagnóstico**.

   A janela **Diagnóstico das regras** é exibida.

4. Preencha os campos na seção **Condições**:

   a. Se desejar testar as regras usadas pelo Kaspersky Endpoint Security para controlar o acesso a um recurso da Web específico, marque a caixa de seleção **Especificar endereço** e insira o endereço do recurso da Web no campo abaixo.

   b. Se desejar testar as regras usadas pelo Kaspersky Endpoint Security para controlar o acesso a recursos da Web por usuários e/ou grupos de usuários especificados, especifique a lista de usuários e/ou grupos de usuários.

   c. Se desejar testar as regras usadas pelo Kaspersky Endpoint Security para controlar o acesso a recursos da Web de categorias de conteúdo e/ou tipos de dados especificados, na lista suspensa **Filtrar conteúdo**, selecione a opção desejada (**Por categorias de conteúdo**, **Por tipos de dados** ou **Por categorias de conteúdo e tipos de dados**).

   d. Se desejar testar as regras incluindo a hora e dia da semana em que a tentativa é feita para acessar o(s) recurso(s) da Web especificado(s) nas condições de diagnóstico das regras, marque a caixa de seleção **Incluir hora da tentativa de acesso**. Especifique o dia da semana e a hora.

5. Clique no botão **Testar**.

A conclusão do teste é seguida de uma mensagem informando a ação realizada pelo Kaspersky Endpoint Security, de acordo com a primeira regra acionada na tentativa de acessar o recurso online especificado (permitir, bloquear ou advertir). A primeira regra acionada é aquela que tem prioridade na lista de regras do Controle da Web que são aplicadas segundo as condições de diagnóstico. A mensagem é exibida à direita do botão **Testar**. A tabela a seguir lista as regras acionadas existentes, especificando a ação do Kaspersky Endpoint Security. As regras são listadas em ordem decrescente de prioridade.

Ativar e desativar a regra de acesso de recurso da Web

Para ativar ou desativar a regra de acesso de recurso da Web:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Controle de Endpoints**, selecione **Controle da Web**.

   À direita da janela, as configurações do componente de Controle da Web serão apresentadas.
3. À direita da janela, selecione a regra que deseja ativar ou desativar.
4. Na coluna **Status**, faça o seguinte:
   - Se desejar ativar o uso da regra, selecione o valor *Ativar*.
   - Se desejar desativar o uso da regra, selecione o valor *Desativar*.
5. Para salvar as alterações, clique no botão **Salvar**.

Migrar regras de acesso a recursos da Web de versões anteriores do aplicativo

Quando a versão anterior do aplicativo ou o Service Pack 1 Maintenance Release 1 for atualizado para Kaspersky Endpoint Security 10 Service Pack 2 for Windows, as regras de acesso de recursos da Web com base nas categorias de conteúdo de recursos da Web são migradas da seguinte forma:

- Recursos da Web baseados em uma ou mais listas de categorias de conteúdo, desde "Fóruns e bate-papo", "Correio na Web" e "Redes sociais" são migrados para a categoria de conteúdo da Web "Mídia em comunicações na Internet".
- As regras de acesso a recursos da Web com base em uma ou mais categorias de conteúdo das listas "Lojas virtuais" e "Sistemas de pagamento" são migradas para a categoria de conteúdo de recursos da Web "Comércio eletrônico".
- Regras de recursos da Web baseadas na categoria de conteúdo "Jogos" são migradas para a categoria de conteúdo "Jogo, loterias, apostas".
- Regras de acesso a recursos da Web baseadas na categoria de conteúdo "Jogos de navegador" são migradas para a categoria de conteúdo "Jogos de computador".
- Regras de acesso a recursos da Web baseadas em categorias de conteúdo que não são descritas acima são migradas sem alterações.

Exportar e importar a lista de endereços de recurso da Web

Se tiver criado uma lista de endereços de recurso da Web em uma regra de acesso de recurso da Web, é possível exportá-la para um arquivo .txt. A seguir, será possível importar a lista deste arquivo para evitar ter de criar uma nova lista de endereços de recurso da Web manualmente ao configurar uma regra de acesso. A opção de exportar e importar a lista de endereços de recurso da Web é útil se, por exemplo, você criar regras de acesso com parâmetros semelhantes.

Para exportar uma lista de endereços de recurso da Web para um arquivo:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Controle de Endpoints**, selecione **Controle da Web**.

   À direita da janela, as configurações do componente de Controle da Web serão apresentadas.
3. Selecione a regra cuja lista de endereços de recurso da Web deseja exportar para um arquivo.
4. Clique no botão **Editar**.

   A janela **Regra de acesso a recursos da Web** é exibida.
5. Se não desejar exportar a lista inteira de endereços de recursos da Web, mas apenas parte desta, selecione os endereços de recurso da Web desejados.
6. À direita do campo com a lista de endereços de recurso da Web, clique no botão  .

   A janela de confirmação abre.
7. Execute uma das seguintes ações:

   - Se desejar exportar apenas os itens selecionados da lista de endereço de recurso da Web, na janela de confirmação, clique no botão **Sim**.
   - Se desejar exportar todos os itens selecionados da lista de endereços de recurso da Web, na janela de confirmação, clique no botão **Não**.

     A janela **Salvar como**, no Microsoft Office, é exibida.
8. Na janela do Microsoft Windows **Salvar como**, selecione o arquivo para o qual deseja exportar a lista de endereços de recurso da Web. Clique no botão **Salvar**.

Para importar a lista de endereços de recursos da Web de um arquivo para uma regra:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Controle de Endpoints**, selecione **Controle da Web**.

   À direita da janela, as configurações do componente de Controle da Web serão apresentadas.
3. Execute uma das seguintes ações:

   - Se desejar criar uma nova regra de acesso de recursos da Web, clique no botão **Adicionar**
   - Selecione a regra de acesso de recursos da Web que deseja editar. Em seguida, clique no botão **Editar**.

   A janela **Regra de acesso a recursos da Web** é exibida.

4. Execute uma das seguintes ações:

   - Ao criar uma nova regra de acesso de recursos da Web, selecione **Para endereços individuais** na lista suspensa **Aplicar aos endereços**.
   - Se estiver editando uma regra de acesso de recursos da Web, vá para a etapa 5 destas instruções.

5. À direita do campo com a lista de endereços de recurso da Web, clique no botão .

   Se estiver criando uma nova regra, a janela padrão do Microsoft Windows **Abrir arquivo** será exibida.

   Se estiver editando uma regra, uma janela solicitando sua confirmação será exibida.

6. Execute uma das seguintes ações:

   - Se estiver editando uma regra de acesso de recursos da Web, vá para a etapa 7 destas instruções.
   - Se estiver editando uma regra de acesso de recursos da Web, execute uma das seguintes operações na janela de confirmação:
     - Se desejar adicionar os itens importados da lista de endereços de recursos da Web aos existentes, clique no botão **Sim**.
     - Se desejar excluir os itens existentes da lista de endereços de recursos da Web e adicionar os importados, clique no botão **Não**.

   A janela **Abrir arquivo**, no Microsoft Windows, é exibida.

7. Na janela do Microsoft Windows **Abrir arquivo**, selecione o arquivo com a lista endereços de recursos da Web a importar.

8. Clique no botão **Abrir**.

9. Na janela **Regra de acesso a recursos da Web**, clique em **OK**.

Editar máscaras de endereços de recurso da Web

Usar uma *máscara de endereço de recurso da Web* (também referida como "máscara de endereço") pode ser útil se precisar inserir vários endereços de recurso da Web semelhantes ao criar uma regra de acesso de recurso da Web. Se for algo bem planejado, uma máscara de endereço pode substituir um grande número de endereços de recurso da Web.

Ao criar uma máscara de endereço, siga as seguintes regras:

1. O caractere * substitui qualquer sequência que contém caractere igual ou superior a zero.

   Por exemplo, se inserir a máscara de endereço *abc*, a regra de acesso é aplicada a todos os recursos da Web que contêm a sequência abc. Exemplo: http://www.example.com/page_0-9abcdef.html.

   Para incluir o caractere * na máscara de endereço, insira o caractere * duas vezes.

2. A sequência de caracteres `www.` no início da máscara de endereço é interpretada como uma sequência `*.`.

   Exemplo: máscara de endereço www.exemplo.com é tratada como *.exemplo.com.

3. Se uma máscara de endereço não começar com o caractere *, o conteúdo da máscara de endereço é equivalente ao mesmo conteúdo com o prefixo `*.`

4. A sequência de caracteres `*.` no início de uma máscara de endereço é interpretada como `*.` ou como uma string vazia.

   Exemplo: a máscara de endereço http://www.*.exemplo.com abrange o endereço http://www2.exemplo.com.

5. Se uma máscara de endereço terminar com um caractere diferente de / ou `*`, o conteúdo da máscara de endereço é equivalente ao mesmo conteúdo com o sufixo `/*`.

   Exemplo: a máscara de endereço http://www.exemplo.com abrange endereços como http://www.exemplo.com/abc, onde a, b e c são quaisquer caracteres.

6. Se uma máscara de endereço terminar com o caractere `/`, o conteúdo da máscara de endereço é equivalente ao mesmo conteúdo com o sufixo `/*.`

7. A sequência de caracteres `/*` no final de uma máscara de endereço é interpretada como `/*` ou como vazia.

8. Endereços de recurso da Web são verificados na máscara de endereço, considerando-se o protocolo (http ou https):

   - Se a máscara de endereço não contém nenhum protocolo de rede, esta abrange endereços com qualquer protocolo de rede.

     Exemplo: a máscara de endereço exemplo.com abrange os endereços http://exemplo.com e https://exemplo.com.

   - Se a máscara de endereço contém um protocolo de rede, esta abrange apenas endereços com o mesmo protocolo de rede da máscara de endereço.

     Exemplo: a máscara de endereço http://*.exemplo.com abrange o endereço http://www.exemplo.com mas não o https://www.exemplo.com.

9. A máscara de endereço que está entre aspas duplas é tratada sem que sejam consideradas qualquer substituições adicionais, exceto quanto ao caractere `*` se este tiver sido incluído inicialmente na máscara de endereço. As regras 5 e 7 não se aplicam a máscaras de endereço colocadas entre aspas duplas (consulte os exemplos 14 - 18 na tabela abaixo).

10. O nome de usuário e a senha, porta de conexão, e distinção entre maiúsculas/minúsculas não são consideradas para fins de comparação com a máscara de endereço de um recurso da Web.

Exemplos de como usar regras para criar máscaras de endereço

Número	Máscara de endereço	Endereço do recurso da Web a verificar	O endereço é abrangido pelo endereço da máscara de endereço	Comentário
1	*.exemplo.com	http://www.123exemplo.com	Não	Consulte a regra 1.
2	*.exemplo.com	http://www.123.exemplo.com	Sim	Consulte a regra 1.
3	*exemplo.com	http://www.123exemplo.com	Sim	Consulte a regra 1.
4	*exemplo.com	http://www.123.exemplo.com	Sim	Consulte a regra 1.
5	http://www.*.exemplo.com	http://www.123exemplo.com	Não	Consulte a regra 1.

6	www.exemplo.com	http://www.exemplo.com	Sim	Consulte as regras 2, 1.
7	www.exemplo.com	https://www.exemplo.com	Sim	Consulte as regras 2, 1.
8	http://www.*.exemplo.com	http://123.exemplo.com	Sim	Consulte as regras 2, 4, 1.
9	www.exemplo.com	http://www.exemplo.com/abc	Sim	Consulte as regras 2, 5, 1.
10	exemplo.com	http://www.exemplo.com	Sim	Consulte as regras 3, 1.
11	http://exemplo.com/	http://exemplo.com/abc	Sim	Consulte a regra 6.
12	http://exemplo.com/*	http://exemplo.com	Sim	Consulte a regra 7.
13	http://exemplo.com	https://exemplo.com	Não	Consulte a regra 8.
14	"exemplo.com"	http://www.exemplo.com	Não	Consulte a regra 9.
15	"http://www.exemplo.com"	http://www.exemplo.com/abc	Não	Consulte a regra 9.
16	"*.exemplo.com"	http://www.exemplo.com	Sim	Consulte as regras 1, 9.
17	"http://www.example.com/*"	http://www.exemplo.com/abc	Sim	Consulte as regras 1, 9.
18	"www.exemplo.com"	http://www.exemplo.com; https://www.exemplo.com	Sim	Consulte as regras 9, 8.
19	www.exemplo.com/abc/123	http://www.exemplo.com/abc	Não	A máscara de endereço contém mais informações além do endereço de um recurso da Web.

Editar modelos de mensagens do Controle da Web

Dependendo do tipo de ação especificada nas propriedades das regras do Controle da Web, o Kaspersky Endpoint Security exibe uma das seguintes mensagens quando os usuários tentam acessar recursos da Internet (o aplicativo substitui a página HTML com a mensagem com a resposta do servidor HTTP):

- Mensagem de aviso. Esta mensagem avisa o usuário que visitar o recurso da Web não é recomendado e/ou viola a política de segurança corporativa. O Kaspersky Endpoint Security exibe uma mensagem de aviso se a opção **Avisar** for selecionada na lista suspensa **Ação** na regra de descrição do recurso da Web.

  Se o usuário considerar que o aviso é um engano, ele pode clicar no link da mensagem de alerta para enviar uma mensagem pré-gerada ao administrador da rede corporativa local.

- Mensagem informando sobre o bloqueio de um recurso da Web. Se a opção **Bloquear** for selecionada na lista suspensa **Ação** nas configurações da regra que descrevem esse recurso da Web, o Kaspersky Endpoint Security exibe uma mensagem de aviso informando que um recurso da Web foi bloqueado.

  Se o usuário considerar que o recurso da Web foi bloqueado por engano, ele pode clicar no link na mensagem de notificação de bloqueio de recurso Web para enviar uma mensagem pré-gerada ao administrador da rede corporativa local.

São fornecidos modelos especiais para uma mensagem de aviso, a mensagem informando que um recurso da Web está bloqueado e a mensagem a ser enviada ao administrador da rede local. É possível modificar o conteúdo.

Para alterar o modelo das mensagens de Controle da Web:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Controle de Endpoints**, selecione **Controle da Web**.

   À direita da janela, as configurações do componente de Controle da Web serão apresentadas.
3. Na parte direita da janela, clique no botão **Modelos**.

   A janela **Modelos de mensagem** é exibida.
4. Execute uma das seguintes ações:

   - Se desejar editar o modelo da mensagem que avisa o usuário para não visitar um recurso da Web, selecione a guia **Aviso**.
   - Se desejar editar o modelo da mensagem que informa o usuário que o acesso a um recurso da Web está bloqueado, selecione a guia **Bloqueio**.
   - Para editar o modelo da mensagem enviada ao administrador, abra a guia **Mensagem para o administrador**.
5. Editar o modelo de mensagem. Você também pode usar a lista suspensa **Variável**, bem como os botões **Padrão** e **Link** (esse botão não está disponível na guia **Mensagem para o administrador**).
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Sensor de endpoints da KATA

As configurações do componente Sensor de endpoints da KATA estão disponíveis somente no Console de administração do Kaspersky Security Center. Para usar esse componente, você deve instalar o plug-in de administração.

Esta seção contém informações sobre o Sensor de endpoints da KATA e instruções sobre como ativar ou desativar esse componente.

Sobre o Sensor de endpoints da KATA

O Sensor de endpoints da KATA é um componente do Kaspersky Anti Targeted Attack Platform. Esta solução é destinada para a detecção rápida de ameaças como ataques visados.

Este componente é instalado nos computadores cliente. Nesses computadores, o componente monitora constantemente os processos, as conexões de rede ativas e os arquivos que são modificados, e retransmite estas informações ao Kaspersky Anti Targeted Attack Platform.

A funcionalidade de componente está disponível nos seguintes sistemas operacionais:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1.
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016

Para obter informações adicionais sobre o Kaspersky Anti Targeted Attack Platform que não é fornecido neste documento, consulte a ajuda do Kaspersky Anti Targeted Attack Platform.

As conexões recebidas para os computadores com o componente Sensor de endpoints da KATA devem ser permitidas do servidor Kaspersky Anti Targeted Attack Platform diretamente, sem um servidor proxy.

Ativar e desativar o componente Sensor de Endpoints da KATA

Para ativar ou desativar o componente Sensor de Endpoints da KATA:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja editar as configurações da política.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.

   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Configurações avançadas**, selecione a subseção **Sensor de Endpoints da KATA**.

7. Execute uma das seguintes ações:

   - Se desejar ativar o Sensor de Endpoints da KATA, marque a caixa de seleção **Sensor de Endpoints da KATA**.

   - Se desejar desativar o Sensor de Endpoints da KATA, desmarque a caixa de seleção **Sensor de Endpoints da KATA**.

8. Se tiver selecionado a caixa de seleção **Sensor de Endpoints da KATA** na etapa anterior, no campo **Endereço do servidor**, especifique o endereço do servidor Kaspersky Anti Targeted Attack Platform composto das seguintes partes:

   a. Nome de protocolo

   b. Endereço IP ou nome de domínio totalmente qualificado (FQDN) do servidor

   c. Caminho até o Coletor de Eventos do Windows no servidor

9. Clique em **OK**.

10. Aplique a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Criptografia de dados

Se o Kaspersky Endpoint Security for instalado em um computador com o Microsoft Windows para Workstations, a funcionalidade de criptografia de dados fica totalmente disponível. Se o Kaspersky Endpoint Security for instalado em um computador com o Microsoft Windows para servidores de arquivo, somente a criptografia de disco rígido usando a tecnologia Criptografia de Unidade de Disco BitLocker fica disponível.

Esta seção contém informações sobre criptografia e descriptografia de discos rígidos, unidades removíveis, arquivos e pastas nas unidades do computador local e fornece instruções sobre como configurar e realizar a criptografia e descriptografia de dados utilizando o Kaspersky Endpoint Security e o plug-in de administração do Kaspersky Endpoint Security.

Se não houver acesso a dados criptografados, consulte as instruções específicas para trabalhar com dados criptografados (Trabalhando com arquivos criptografados no caso de funcionalidade de criptografia de arquivo limitada, Trabalhando com dispositivos criptografados caso o acesso a eles não exista).

Ativar a exibição das configurações de criptografia na política do Kaspersky Security Center

Para ativar a exibição das configurações de criptografia na política do Kaspersky Security Center:

1. Abra o Console de Administração do Kaspersky Security Center.
2. No menu de contexto do nó **Servidor de Administração – <Nome do computador>** da árvore do Console de Administração, selecione **Exibir → Configurações da interface**.

   A janela **Configurações da interface** é exibida.
3. Na janela **Configurações de interface**, selecione a caixa de seleção **Exibir criptografia e proteção de dados**.
4. Clique em **OK**.

Sobre a criptografia de dados

O Kaspersky Endpoint Security permite a criptografia de arquivos e pastas armazenados em unidades locais e removíveis ou em unidades removíveis e discos rígidos inteiros. A criptografia de dados minimiza o risco de vazamento de informação que pode resultar quando um computador portátil, uma unidade removível ou um disco rígido é perdido ou roubado ou quando os dados são acessados por usuários ou aplicativos não autorizados.

Se a licença expirou, o aplicativo não criptografa novos dados, os dados criptografados antigos permanecem criptografados e disponíveis para uso. Neste caso, a criptografia de novos dados exige que o programa seja ativado com uma nova licença que permite o uso da criptografia.

Se a sua licença tiver expirado ou o Contrato de Licença do Usuário Final tiver sido violado, a chave, o Kaspersky Endpoint Security ou os componentes de criptografia tiverem sido removidos, o status de criptografado dos arquivos criptografados anteriormente não é garantido. Isso porque alguns aplicativos, como o Microsoft Office Word, criam cópias temporárias de arquivos durante a edição. Quando o arquivo original é salvo, a cópia temporária substitui o arquivo original. Por conseguinte, em um computador que não tem funcionalidade de criptografia ou essa funcionalidade fica inacessível, o arquivo permanece não criptografado.

O Kaspersky Endpoint Security oferece os seguintes aspectos de proteção de dados:

- **Criptografia de arquivos em unidades de computadores locais**. Você pode compilar listas de arquivos por extensão ou por grupos de extensões e listas de pastas armazenadas em unidades do computador local, bem como criar regras para criptografar arquivos criados por aplicativos específicos. Depois que uma política do Kaspersky Security Center é aplicada, o Kaspersky Endpoint Security criptografa e descriptografa os seguintes arquivos:

  - Arquivos individualmente adicionados a listas de criptografia e descriptografia.
  - Arquivos guardados em pastas adicionadas a listas de criptografia e descriptografia.
  - arquivos criados por aplicativos separados.

  Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

- **Criptografia de unidades removíveis**. Você pode especificar uma regra de criptografia padrão a ser utilizada pelo aplicativo igualmente em todas as unidades removíveis, ou especificar as regras de criptografia para unidades removíveis específicas.

  A regra de criptografia padrão tem uma prioridade mais baixa do que as regras de criptografia criadas para unidades removíveis individuais. Regras de criptografia criadas para unidades removíveis do modelo de dispositivo especificado têm uma prioridade mais baixa do que as regras de criptografia criadas para unidades removíveis com a ID de dispositivo especificada.

  Para selecionar a regra de criptografia para arquivos em uma unidade removível, o Kaspersky Endpoint Security verifica se o modelo do dispositivo e a ID são conhecidos. O aplicativo então executa uma das seguintes operações:

  - Se apenas o modelo do dispositivo for conhecido, o aplicativo usa a regra de criptografia (se houver) criada para unidades removíveis com um modelo de dispositivo específico.
  - Se a ID do dispositivo for conhecida, o aplicativo usa a regra de criptografia (se houver) criada para unidades removíveis com uma ID de dispositivo específica.
  - Se o modelo e a ID do dispositivo forem conhecidos, o aplicativo usa a regra de criptografia (se houver) criada para unidades removíveis com uma ID de dispositivo específica. Se nenhuma regra existir, mas houver uma regra de criptografia criada para unidades removíveis com o modelo de dispositivo específico, o aplicativo aplica essa regra. Se nenhuma regra de criptografia for especificada para a ID de dispositivo específica nem para o modelo de dispositivo específico, o aplicativo aplica a regra de criptografia padrão.
  - Se nem o modelo nem o ID do dispositivo forem conhecidos, o aplicativo usa a regra de criptografia padrão.

  O aplicativo permite que você prepare uma unidade removível para utilizar dados armazenados no modo portátil. Depois de ativar o modo portátil, você pode acessar os arquivos criptografados em unidades removíveis conectadas a um computador sem a funcionalidade de criptografia.

  O aplicativo executa a ação especificada na regra de criptografada quando a política do Kaspersky Security Center é aplicada.

- **Gerenciar regras de acesso do aplicativo a arquivos criptografados**. Para qualquer aplicativo, você pode criar uma regra de acesso ao arquivo criptografado que bloqueia o acesso a arquivos criptografados ou permite o acesso a arquivos criptografados somente como ciphertext, que é uma sequência de caracteres obtida quando a criptografia é aplicada.

- **Criar arquivos compactados criptografados**. Você pode criar arquivos compactados criptografados e proteger o acesso a esses arquivos com uma senha. O conteúdo dos arquivos compactados criptografados pode ser acessado apenas com a introdução da senha com a qual você protegeu o acesso a esses arquivos. Tais arquivos compactados podem ser transmitidos com segurança pela rede ou em unidades removíveis.

- **Criptografia de discos rígidos**. Você pode selecionar uma tecnologia de criptografia: o Kaspersky Disk Encryption ou Criptografia de Unidade de Disco BitLocker (a partir daqui também mencionada como simplesmente "BitLocker").

  BitLocker é uma tecnologia integrante do sistema operacional Windows. Se um computador for equipado com Trusted Platform Module (TPM), o BitLocker utiliza esse recurso para guardar chaves de recuperação que fornecem o acesso a um disco rígido criptografado. Quando o computador é iniciado, o BitLocker solicita as chaves de recuperação de disco rígido do Trusted Platform Module e desbloqueia a unidade. Você pode configurar o uso de uma senha e/ou código PIN para acessar chaves de recuperação.

  Você pode especificar o padrão da regra de criptografia e criar uma lista de discos rígidos a serem excluídos da criptografia. O Kaspersky Endpoint Security criptografa discos rígidos, setor por setor, quando a política do Kaspersky Security Center é aplicada. O aplicativo criptografa todas as partições lógicas dos discos rígidos simultaneamente. Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

  Após a criptografia dos discos rígidos do sistema, na próxima inicialização do sistema o usuário deve concluir a autenticação usando o Agente de Autenticação antes que os discos rígidos possam ser acessados e o sistema operacional seja carregado. Isso requer inserir a senha do token ou cartão inteligente conectado ao computador ou o nome de usuário e a senha da conta do Agente de Autenticação criada pelo administrador de rede local que usa tarefas de gerenciamento de contas do Agente de Autenticação. Estas contas são baseadas nas contas do Microsoft Windows com a qual os usuários fazem login no sistema operacional. Você pode gerenciar as contas do Agente de Autenticação e usar a tecnologia de login único (SSO), que permite fazer login no sistema operacional automaticamente, usando o nome de usuário e a senha da conta do Agente de Autenticação.

  > Se você fizer o backup do computador, a seguir criptografar os dados do computador e após isso restaurar a cópia de backup do computador e então criptografar os dados do computador novamente, o Kaspersky Endpoint Security cria duplicatas das contas do Agente de Autenticação. Para remover as contas duplicadas, utilize o utilitário klmover com a chave `-dupfix`. O utilitário klmover está incluído na compilação do Kaspersky Security Center. Você pode ler mais sobre a sua operação no *Guia de Administrador do Kaspersky Security Center*.

  > Quando uma versão do aplicativo é atualizada para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, a lista de contas do Agente de Autenticação não é salva.

  O acesso a discos rígidos criptografados só é possível em computadores em que está instalado o Kaspersky Endpoint Security com funcionalidade de criptografia de disco rígido. Esta precaução minimiza o risco de vazamento de dados de um disco rígido criptografado quando for feita uma tentativa de acesso fora da rede local da empresa.

Para criptografar discos rígidos e unidades removíveis, você pode usar o modo **Criptografar somente espaço usado em disco**. Recomenda-se somente usar esta função para novos dispositivos que não foram anteriormente usados. Se você estiver aplicando a criptografia em um dispositivo que já está em uso, recomenda-se criptografar o dispositivo inteiro. Isto assegura que todos os dados sejam protegidos, até os dados excluídos que ainda podem conter informações recuperáveis.

Antes da criptografia começar, o Kaspersky Endpoint Security obtém o mapa de setores de sistema de arquivos. A primeira onda da criptografia inclui setores que são ocupados por arquivos no momento em que a criptografia é iniciada. A segunda onda da criptografia inclui setores que foram gravados depois que a criptografia começou. Depois que a criptografia é concluída, todos os setores que contêm dados estão criptografados.

Depois que a criptografia é concluída e um usuário exclui um arquivo, os setores que guardaram o arquivo apagado ficam disponíveis para guardar novas informações no nível de sistema de arquivos, mas permanecem criptografados. Assim, à medida que novos arquivos são gravados em um novo dispositivo durante a inicialização normal da criptografia com a função **Criptografar somente espaço usado em disco** ativada no computador, após algum tempo, todos os setores serão criptografados.

Os dados necessários para a descriptografia de arquivos é fornecido pelo Servidor de Administração do Kaspersky Security Center que controlou o computador no momento da criptografia. Se o computador com arquivos criptografados se encontrar sob controle de outro Servidor de Administração por qualquer motivo e os arquivos criptografados não tiverem sido acessados vez alguma, o acesso pode ser obtido de uma das seguintes formas:

- solicitando o acesso a objetos criptografados do administrador da rede local;
- restaurando o acesso a dispositivos criptografados usando o Utilitário de Restauração;
- Restaurando a configuração do Servidor de Administração do Kaspersky Security Center que controlou o computador no momento da criptografia a partir de uma cópia de backup, e utilizando esta configuração no Servidor de Administração que agora controla o computador com os objetos criptografados.

O aplicativo cria arquivos de serviço durante a criptografia. É necessário cerca de dois ou três por cento de espaço livre não fragmentado no disco rígido para armazená-los. Se não houver espaço livre não fragmentado suficiente no disco rígido, a criptografia não será iniciada até que você libere espaço suficiente.

A compatibilidade entre a funcionalidade de criptografia do Kaspersky Endpoint Security e do Kaspersky Anti-Virus para UEFI não é suportada. A criptografia de discos rígidos em computadores com o Kaspersky Anti-Virus para UEFI instalado torna o Kaspersky Anti-Virus para UEFI inutilizável.

Limitações de funcionalidades da criptografia

Criar novas partições em discos rígidos criptografados, assim como formatar as partições existentes dos discos rígidos criptografados, pode causar a perda de dados nestes discos rígidos.

A tecnologia de criptografia de disco rígido que usa Kaspersky Disk Encryption está indisponível para discos rígidos que não atendem aos requisitos de software e hardware.

O Kaspersky Endpoint Security não suporta as seguintes configurações:

- O carregador de inicialização é localizado em uma unidade enquanto o sistema operacional está em uma unidade diferente.
- O sistema contém o software integrado do padrão de UEFI 32.
- Intel® Rapid Start Technology e as unidades que têm uma partição de hibernação mesmo quando o Intel® Rapid Start Technology está desativado.

- Unidades em formato de MBR com mais de quatro partições estendidas.
- O arquivo de troca localizado em uma unidade de não-sistema.
- Sistema de inicialização múltipla com vários sistemas operacionais simultaneamente instalados.
- As partições dinâmicas (somente partições primárias são suportadas).
- Unidades com espaço disponível não fragmentado livre de menos de 2%.
- Unidades com um tamanho de setor diferente de 512 bytes ou 4096 bytes que emulam 512 bytes.
- Unidades híbridas.

Alterar o algoritmo de criptografia

O algoritmo de criptografia usado por Kaspersky Endpoint Security para a criptografia de dados depende das bibliotecas de criptografia que estão incluídas no kit de distribuição.

Para alterar o algoritmo de criptografia:

1. Descriptografe os objetos que o Kaspersky Endpoint Security criptografou antes de começar a modificar o algoritmo de criptografia.

   Depois que o algoritmo de criptografia é modificado, os objetos que foram anteriormente criptografados tornam-se indisponíveis.

2. Remova o Kaspersky Endpoint Security.
3. Instale o Kaspersky Endpoint Security do kit de distribuição que contém bibliotecas de criptografia de contas de bit diferentes.

Ativar a tecnologia de login único (SSO)

A tecnologia de login único (SSO) é incompatível com provedores terceiros de credenciais de conta.

Para ativar a tecnologia de login único (SSO):

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja ativar a tecnologia de login único (SSO).
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

- No menu de contexto da política, selecione **Propriedades**.
- Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Criptografia de dados**, selecione a subseção **Configurações comuns de criptografia**.
7. Na subseção **Configurações comuns de criptografia**, clique no botão **Configurar** na seção **Configurações da senha**.

   É exibida a guia **Agente de Autenticação** da janela **Configurações da senha de criptografia**.
8. Marque a caixa de seleção **Usar a tecnologia de login único (SSO)**.
9. Clique em **OK**.
10. Para salvar as alterações, na janela **Propriedades: <Nome de política>**, clique em **OK**.
11. Aplique a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Considerações especiais da criptografia de arquivos

Ao utilizar a funcionalidade de criptografia de arquivos, considere os seguintes pontos:

- A política do Kaspersky Security Center com configurações predefinidas para criptografia de unidades removíveis é formada por um grupo específico de computadores gerenciados. Portanto, o resultado da política de criptografia/descriptografia do aplicativo em unidades removíveis depende do computador em que a unidade removível for conectada.
- O Kaspersky Endpoint Security não criptografa/descriptografa arquivos com status de somente leitura armazenados em unidades removíveis.
- O Kaspersky Endpoint Security criptografa/descriptografa arquivos em pastas predefinidas apenas para perfis de usuários locais do sistema operacional. O Kaspersky Endpoint Security não criptografa/descriptografa arquivos em pastas predefinidas do perfil de usuário móvel, perfil de usuário obrigatório, perfil de usuário temporário e em pastas redirecionadas. A lista de pastas padrão recomendada pela Kaspersky para criptografia inclui as seguintes pastas:
  - Meus Documentos
  - Favoritos
  - Cookies
  - Área de Trabalho
  - Arquivos temporários do Internet Explorer
  - Arquivos temporários
  - Arquivos do Outlook

- O Kaspersky Endpoint Security não criptografa arquivos e pastas quando isso pode danificar o sistema operacional e os aplicativos instalados. Por exemplo, os arquivos e pastas a seguir com todas as pastas aninhadas estão na lista de exclusões da criptografia:
  - %WINDIR%.
  - %PROGRAMFILES%, %PROGRAMFILES(X86)%.
  - Arquivos de registro do Windows.

  A lista de exclusões da criptografia não pode ser visualizada nem editada. Enquanto arquivos e pasta na lista de exclusões da criptografia puderem ser adicionados à lista de criptografia, eles não serão criptografados durante uma tarefa de criptografia de arquivos e pastas.
- Os tipos de dispositivo a seguir têm suporte como unidades removíveis:
  - Mídia de dados conectadas por barramento USB
  - discos rígidos conectados por barramento USB e FireWire
  - unidades SSD conectadas por barramento USB e FireWire

Criptografia de arquivos em unidades de computadores locais

A criptografia de arquivos em computadores locais estará disponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado com o Microsoft Windows para estações de trabalho. A criptografia de arquivos em unidades de computadores locais não estará disponível se o Kaspersky Endpoint Security estiver instalado num computador que seja executado com o Microsoft Windows para servidores de arquivos.

Esta seção abrange a criptografia de arquivos em unidades de computadores locais e oferece instruções sobre como configurar e executar a criptografia de arquivos em unidades de computadores locais com o Kaspersky Endpoint Security e com o Plug-in de Console Kaspersky Endpoint Security.

Criptografia de arquivos em unidades de computadores locais

Para criptografar arquivos em unidades locais:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados**, na árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja editar as configurações de criptografia de arquivos em unidades locais.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

- No menu de contexto da política, selecione **Propriedades**.
- Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de arquivos e pastas**.
7. À direita da janela, selecione a guia **Criptografia**.
8. Na lista suspensa **Modo de criptografia**, selecione o item **Regras padrão**.
9. Na guia **Criptografia**, clique no botão **Adicionar**, e na lista suspensa selecione um dos seguintes itens:
   a. Selecione o item de **Pastas predefinidas** para adicionar arquivos de pastas de perfis de usuário local sugeridos por peritos da Kaspersky a uma regra de criptografia.
      A janela **Selecionar pastas predefinidas** abre.
   b. Selecione o item **Pasta personalizada** para adicionar um caminho de pasta manualmente inserido a uma regra de criptografia.
      A janela **Adicionar pasta personalizada** abre.
   c. Selecione o item **Arquivos por extensão** para adicionar extensões de arquivo a uma regra de criptografia. O Kaspersky Endpoint Security criptografa arquivos com as extensões especificadas em todas as unidades do computador.
      A janela **Adicionar / editar a lista de extensões de arquivos** abre.
   d. Selecione o item **Arquivos por grupo(s) de extensões** para adicionar grupos de extensões de arquivo a uma regra de criptografia. O Kaspersky Endpoint Security criptografa arquivos apresentam as extensões listadas nos grupos de extensões em todas as unidades locais do computador.
      A janela **Selecione grupos de extensões de arquivo** abre.
10. Para salvar as alterações, na janela **Propriedades: <Nome de política>**, clique em **OK**.
11. Aplique a política.
    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Logo que a política é aplicada, o Kaspersky Endpoint Security criptografa os arquivos que estão incluídos na regra de criptografia e não incluídos na regra de descriptografia.

Se o mesmo arquivo foi adicionado à lista de criptografia e descriptografia, o Kaspersky Endpoint Security não o criptografa se ele não estiver criptografado e o descriptografa se ele estiver criptografado.

O Kaspersky Endpoint Security criptografa arquivos não criptografados se as suas propriedades (caminho de arquivo/nome de arquivo/extensão de arquivo) ainda atenderem aos critérios da regra e criptografia depois da modificação.

O Kaspersky Endpoint Security adia a criptografia de arquivos abertos até que eles sejam fechados.

Quando o usuário cria um novo arquivo cujas propriedades atendem aos critérios da regra de criptografia, o Kaspersky Endpoint Security criptografa o arquivo logo que ele é aberto.

Se você mover um arquivo criptografado para outra pasta na unidade local, o arquivo permanece criptografado independente da pasta estar ou não na regra de criptografia.

Formar regras de acesso a arquivos criptografados para aplicativos

Para formar regras de acesso a arquivos criptografados para aplicativos:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados**, na árvore do Console de Administração, abra a pasta com o nome do grupo de administração relevante para o qual você deseja configurar as regras de acesso a arquivos criptografados para aplicativos.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de arquivos e pastas**.
7. Na lista suspensa **Modo de criptografia**, selecione o item **Regras padrão**.

   As regras de acesso são aplicadas somente quando em modo de **Regras padrão**. Depois de aplicar regras de acesso no modo **Regras Padrão**, se você alterar para o modo **Manter inalterado**, o Kaspersky Endpoint Security ignorará todas as regras de acesso. Todos os aplicativos terão acesso a todos os arquivos criptografados.

8. Na parte direita da janela, selecione a guia **Regras para aplicativos**.
9. Se desejar selecionar aplicativos exclusivamente na lista do Kaspersky Security Center, clique no botão **Adicionar** e, na lista suspensa, selecione o item **Aplicativos da lista do Kaspersky Security Center**.

   A janela **Adicionar aplicativos da lista do Kaspersky Security Center** é exibida.

   Faça o seguinte:

   a. Especifique os filtros para restringir a lista de aplicativos na tabela. Para fazer isso, especifique os valores dos parâmetros **Aplicativo**, **Fornecedor** e **Período adicionado** e todas as caixas de seleção da seção **Grupo**.

   b. Clique no botão **Atualizar**.

      A tabela lista os aplicativos que correspondem aos filtros aplicados.

   c. Na coluna **Aplicativos**, marque as caixas de seleção ao lado dos aplicativos para os quais você deseja formar as regras de acesso a arquivos criptografados.

   d. Na lista suspensa **Regra para o(s) aplicativo(s)**, selecione a regra que determinará o acesso de aplicativos a arquivos criptografados.

e. Na lista suspensa **Ações para aplicativos que foram selecionados anteriormente**, selecione a ação a ser executada pelo Kaspersky Endpoint Security para as regras de acesso que foram formadas anteriormente para os aplicativos já mencionados.

f. Clique em **OK**.

Os detalhes de uma regra de acesso a arquivos criptografados para aplicativos aparecem em uma tabela na guia **Regras para aplicativos**.

10. Se desejar selecionar manualmente os aplicativos, clique no botão **Adicionar** e, na lista suspensa, selecione o item **Aplicativos personalizados**.

    A janela **Adicionar / editar os nomes dos arquivos executáveis dos aplicativos** é exibida.

    Faça o seguinte:

    a. No campo de entrada, digite o nomes ou uma lista de nomes de arquivos de aplicativos executáveis, incluindo suas extensões.

       Para adicionar nomes de arquivos executáveis dos aplicativos a partir da lista do Kaspersky Security Center, clique no botão **Adicionar da lista do Kaspersky Security Center**.

    b. Se necessário, no campo **Descrição**, insira uma descrição da lista de aplicativos.

    c. Na lista suspensa **Regra para o(s) aplicativo(s)**, selecione a regra que determinará o acesso de aplicativos a arquivos criptografados.

    d. Clique em **OK**.

    Os detalhes de uma regra de acesso a arquivos criptografados para aplicativos aparecem em uma tabela na guia **Regras para aplicativos**.

11. Clique em **OK** para salvar as alterações.

Criptografar arquivos que são criados ou modificados por aplicativos específicos

Você pode criar uma regra segundo a qual o Kaspersky Endpoint Security criptografa todos os arquivos criados ou modificados pelos aplicativos especificados na regra.

> Os arquivos que foram criados ou modificados pelos aplicativos especificados antes da regra de criptografia ter sido aplicada não serão criptografados.

Para configurar a criptografia de arquivos que são criados ou modificados por aplicativos específicos:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados**, na árvore do Console de Administração, abra a pasta com o nome do grupo de administração relevante para o qual deseja editar as configurações de criptografia criadas por aplicativos específicos.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de arquivos e pastas**.

7. Na lista suspensa **Modo de criptografia**, selecione o item **Regras padrão**.

   As regras de criptografia são aplicadas somente no modo de **Regras padrão**. Depois de aplicar as regras de criptografia no modo de **Regras padrão**, se você mudar para modo **Manter inalterado**, o Kaspersky Endpoint Security ignorará todas as regras de criptografia. Os arquivos que foram anteriormente criptografados permanecerão criptografados.

8. Na parte direita da janela, selecione a guia **Regras para aplicativos**.

9. Se desejar selecionar aplicativos exclusivamente na lista do Kaspersky Security Center, clique no botão **Adicionar** e, na lista suspensa, selecione o item **Aplicativos da lista do Kaspersky Security Center**.

   A janela **Adicionar aplicativos da lista do Kaspersky Security Center** é exibida.

   Faça o seguinte:

   a. Especifique os filtros para restringir a lista de aplicativos na tabela. Para fazer isso, especifique os valores dos parâmetros **Aplicativo**, **Fornecedor** e **Período adicionado** e todas as caixas de seleção da seção **Grupo**.

   b. Clique no botão **Atualizar**.

      A tabela lista os aplicativos que correspondem aos filtros aplicados.

   c. Na coluna **Aplicativo**, marque as caixas de seleção em frente dos aplicativos cujos arquivos criados precisam ser criptografados.

   d. Na lista suspensa **Regra para o(s) aplicativo(s)**, selecione **Criptografar todos os arquivos criados**.

   e. Na lista suspensa **Ações para aplicativos que foram selecionados anteriormente**, selecione a ação a ser executada pelo Kaspersky Endpoint Security nas regras de criptografia de arquivos formadas anteriormente para os já mencionados aplicativos.

   f. Clique em **OK**.

   As informações sobre a regra de criptografia de arquivos criados ou modificados pelos aplicativos selecionados aparecem na tabela na guia **Regras para aplicativos**.

10. Se desejar selecionar manualmente os aplicativos, clique no botão **Adicionar** e, na lista suspensa, selecione o item **Aplicativos personalizados**.

    A janela **Adicionar / editar os nomes dos arquivos executáveis dos aplicativos** é exibida.

    Faça o seguinte:

    a. No campo de entrada, digite o nomes ou uma lista de nomes de arquivos de aplicativos executáveis, incluindo suas extensões.

       Para adicionar nomes de arquivos executáveis dos aplicativos a partir da lista do Kaspersky Security Center, clique no botão **Adicionar da lista do Kaspersky Security Center**.

b. Se necessário, no campo **Descrição**, insira uma descrição da lista de aplicativos.

c. Na lista suspensa **Regra para o(s) aplicativo(s)**, selecione **Criptografar todos os arquivos criados**.

d. Clique em **OK**.

As informações sobre a regra de criptografia de arquivos criados ou modificados pelos aplicativos selecionados aparecem na tabela na guia **Regras para aplicativos**.

11. Clique em **OK** para salvar as alterações.

Gerar uma regra de descriptografia

Para gerar uma regra de descriptografia:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados**, na árvore do Console de Administração, abra a pasta com o nome do grupo de administração em que deseja formar uma lista de arquivos a serem descriptografados.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de arquivos e pastas**.
7. Na parte direita da janela, selecione a guia **Descriptografia**.
8. Na lista suspensa **Modo de criptografia**, selecione o item **Regras padrão**.
9. Na guia **Descriptografia**, clique no botão **Adicionar** e, na lista suspensa, selecione um dos seguintes itens:

   a. Selecione o item **Pastas predefinidas** para adicionar arquivos de pastas de perfis de usuário local sugeridos por peritos do Kaspersky a uma regra de descriptografia.

   A janela **Selecionar pastas predefinidas** abre.

   b. Selecione o item **Pasta personalizada** para adicionar um caminho de pasta inserido manualmente a uma regra de descriptografia.

   A janela **Adicionar pasta personalizada** abre.

   c. Selecione **Arquivos por extensão** para adicionar extensões de arquivo a uma regra de descriptografia. O Kaspersky Endpoint Security não criptografa arquivos com as extensões especificadas em todas as unidades do computador.

   A janela **Adicionar / editar a lista de extensões de arquivos** abre.

d. Selecionar o item **Arquivos por grupo(s) de extensões** para adicionar grupos de extensões de arquivo a uma regra de descriptografia. O Kaspersky Endpoint Security não criptografa arquivos que apresentam as extensões listadas nos grupos de extensões em todas as unidades locais do computador.

A janela **Selecione grupos de extensões de arquivo** abre.

10. Para salvar as alterações, na janela **Propriedades: <Nome de política>**, clique em **OK**.

11. Aplique a política.

Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Se o mesmo arquivo foi adicionado à lista de criptografia e descriptografia, o Kaspersky Endpoint Security não o criptografa se ele não estiver criptografado e o descriptografa se ele estiver criptografado.

Descriptografar arquivos em unidades de computadores locais

Para descriptografar arquivos em unidades locais:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados**, na árvore do Console de administração, abra a pasta com o nome do grupo de administração para o qual deseja editar as configurações de descriptografia de arquivos em unidades locais.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

- No menu de contexto da política, selecione **Propriedades**.

- Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de arquivos e pastas**.

7. À direita da janela, selecione a guia **Criptografia**.

8. Remova da lista de criptografia os arquivos e pastas que você deseja descriptografar. Para isso, selecione os arquivos e o item **Excluir regra e descriptografar arquivos** no menu de contexto do botão **Remover**.

Você pode excluir vários itens da lista de criptografia de uma só vez. Para isso, enquanto pressiona a tecla **CTRL**, selecione os arquivos de que precisa clicando neles com o botão esquerdo do mouse e selecione o item **Excluir regra e descriptografar arquivos** no menu de contexto do botão **Remover**.

Os arquivos e pastas removidos da lista de criptografia são automaticamente adicionados à lista de descriptografia.

9. Forme a lista de descriptografia.

10. Para salvar as alterações, na janela **Propriedades: <Nome de política>**, clique em **OK**.

11. Aplique a política.

Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Assim que a política é aplicada, o Kaspersky Endpoint Security descriptografa os arquivos criptografados adicionados à lista de descriptografia.

O Kaspersky Endpoint Security descriptografará os arquivos criptografados se seus parâmetros (caminho/nome/extensão do arquivo) se alterarem para corresponder aos parâmetros dos objetos que foram adicionados à lista de descriptografia.

O Kaspersky Endpoint Security adia a descriptografia de arquivos abertos até que eles sejam fechados.

Criar pacotes criptografados

O Kaspersky Endpoint Security não executa a compressão de arquivos ao criar um pacote criptografado.

Para criar um pacote criptografado:

1. Em um computador em que o Kaspersky Endpoint Security esteja instalado e a funcionalidade de criptografia esteja ativada, use qualquer gerenciador de arquivos para selecionar arquivos e/ou pastas que você deseje adicionar a um pacote criptografado. Clique com o botão direito do mouse para abrir o menu de contexto.

2. No menu de contexto, selecione **Adicionar ao pacote criptografado**.

   A caixa de diálogo padrão do Microsoft Windows **Escolha o caminho para salvar o pacote criptografado** é exibida.

3. Na caixa de diálogo padrão do Microsoft Windows **Escolha o caminho para salvar o pacote criptografado**, selecione um destino para salvar o pacote criptografado no disco removível. Clique no botão **Salvar**.

   A janela **Adicionar ao pacote criptografado** é exibida.

4. Na janela **Adicionar ao pacote criptografado**, digite e confirme a senha.

5. Clique no botão **Criar**.

   O processo de criação do pacote criptografado é iniciado. Quando o processo é concluído, é criado um pacote criptografado autoextraível protegido por senha na pasta de destino selecionada no disco removível.

Se você cancelar a criação de um pacote criptografado, o Kaspersky Endpoint Security executará as seguintes operações:

1. Encerra o processo de cópia de arquivos para o pacote e encerra todas as operações de criptografia de pacotes, se houver.

2. Remove todos os arquivos temporários produzidos no processo de criação e criptografia do pacote e do arquivo do pacote criptografado em si.

3. Notifica o usuário que o processo de criação do pacote criptografado foi forçadamente encerrado.

Extrair pacotes criptografados

Para extrair um pacote criptografado:

1. Em qualquer gerenciador de arquivos, selecione um pacote criptografado. Clique para iniciar o Assistente de Desempacotamento.

   A janela **Inserir senha** é exibida.

2. Insira a senha que protege o pacote criptografado.

3. Na janela **Inserir senha**, clique em **OK**.

   Se a entrada de senha tiver êxito, a caixa de diálogo padrão **Procurar** do Microsoft Windows será exibida.

4. Na caixa de diálogo padrão do Microsoft Windows **Procurar**, selecione a pasta de destino para extrair o pacote criptografado e clique em **OK**.

   É iniciado o processo de extração do pacote criptografado para a pasta de destino.

Se o pacote criptografado tiver sido extraído anteriormente para a pasta de destino especificada, os arquivos existentes na pasta serão substituídos.

Se você cancelar a extração de um pacote criptografado, o Kaspersky Endpoint Security executará as seguintes operações:

1. Interrompe o processo de descriptografia do pacote e encerra todas as operações de cópia de arquivos do pacote criptografado, se esta operação estiver em andamento.

2. Exclui todos os arquivos temporários criados no decorrer da descriptografia e extração do pacote, bem como todos os arquivos que já tiverem sido copiados do pacote criptografado para a pasta de destino.

3. Notifica o usuário que o processo de extração do pacote criptografado foi forçadamente encerrado.

Criptografia de unidades removíveis

A criptografia de unidades removíveis está disponível se o Kaspersky Endpoint Security estiver instalado em um computador que seja executado com o Microsoft Windows para estações de trabalho. A criptografia de unidades removíveis não está disponível se o Kaspersky Endpoint Security for instalado em um computador que executa em Microsoft Windows de servidores de arquivos.

Essa seção contém informações sobre a Criptografia de unidades removíveis e instruções sobre como configurar e realizar a Criptografia de unidades removíveis utilizando o Kaspersky Endpoint Security e o plug-in de administração do Kaspersky Endpoint Security.

Iniciar a criptografia de unidades removíveis

Para criptografar unidades removíveis:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja configurar a criptografia de unidades removíveis.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.

   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de unidades removíveis**.

7. Na lista suspensa **Modo de criptografia**, selecione a ação padrão a ser executada pelo Kaspersky Endpoint Security em todas as unidades removíveis que são conectadas aos computadores no grupo de administração selecionado:

   - **Criptografar toda a unidade removível**. Se esse item estiver selecionado, ao aplicar a política do Kaspersky Security Center com as configurações de criptografia especificadas para unidades removíveis, o Kaspersky Endpoint Security criptografa o conteúdo das unidades removíveis, setor por setor. Como resultado, o aplicativo criptografa não apenas arquivos armazenados nas unidades removíveis mas também sistemas de arquivos de unidades removíveis, incluindo nomes de arquivos e estruturas de pastas. O Kaspersky Endpoint Security não criptografa novamente unidades removíveis que já foram criptografadas.

     Este cenário de criptografia é ativado pela funcionalidade de criptografia de disco rígido do Kaspersky Endpoint Security.

   - **Criptografar todos os arquivos**. Se esse item for selecionado ao aplicar a política do Kaspersky Security Center com as configurações de criptografia especificadas para unidades removíveis, o Kaspersky Endpoint Security criptografa todos os arquivos armazenados em unidades removíveis. O Kaspersky Endpoint Security não criptografa arquivos que já foram criptografados. O aplicativo não criptografa os sistemas de arquivo de unidades removíveis, incluindo os nomes de arquivos criptografados e estruturas de pastas.

   - **Criptografar apenas novos arquivos**. Se esse item for selecionado ao aplicar a política do Kaspersky Security Center com as configurações de criptografia especificadas para unidades removíveis, o Kaspersky Endpoint Security criptografa somente aqueles arquivos que foram adicionados a unidades removíveis ou armazenados em unidades removíveis e modificados depois que a política do Kaspersky Security Center foi aplicada pela última vez.

   - **Descriptografar toda a unidade removível**. Se esse item estiver selecionado, ao aplicar a política do Kaspersky Security Center com as configurações de criptografia especificadas para unidades removíveis, o Kaspersky Endpoint Security descriptografa todos os arquivos criptografados e armazenados nas unidades removíveis, bem como os sistemas de arquivo das unidades removíveis se elas tiverem sido criptografadas anteriormente.

     Este cenário de criptografia é possível tanto pela funcionalidade de criptografia de arquivos quanto pela funcionalidade de criptografia de discos rígidos do Kaspersky Endpoint Security.

   - **Manter inalterado**. Se esse item for selecionado ao aplicar a política do Kaspersky Security Center com as configurações de criptografia especificadas para unidades removíveis, o Kaspersky Endpoint Security não criptografa ou descriptografa os arquivos das unidades removíveis.

8. Crie regras de criptografia para arquivos em unidades removíveis cujos conteúdos você deseja criptografar.

9. Aplique a política.

Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Assim que a política for aplicada, quando o usuário conectar uma unidade removível ou se uma unidade removível já estiver conectada, o Kaspersky Endpoint Security notifica o usuário de que a unidade removível está sujeita a à regra de criptografia em que os dados armazenados serão criptografados.

Se a regra *Manter inalterado* for especificada para a criptografia de dados em um disco removível, o aplicativo não exibe notificações ao usuário.

O aplicativo avisa o usuário que o processo de criptografia pode demorar algum tempo.

O aplicativo solicita que o usuário confirme a operação de criptografia e executa as ações a seguir:

- Criptografa dados de acordo com as políticas de configuração, caso o usuário consinta com a criptografia.
- Mantém os dados não criptografados se o usuário rejeitar a criptografia, e limita o acesso a arquivos de unidades removíveis como somente leitura.
- Mantém os dados não criptografados se o usuário ignorar a solicitação de criptografia, limita o acesso a arquivos de unidades removíveis como somente leitura e solicita que o usuário confirme novamente a criptografia de dados na próxima vez que a política do Kaspersky Security Center for aplicada ou quando uma unidade removível for conectada.

A política do Kaspersky Security Center com configurações predefinidas para criptografia de dados em unidades removíveis é formada por um grupo específico de computadores gerenciados. Portanto, o resultado da criptografia de dados em unidades removíveis depende do computador em que a unidade removível for conectado.

Se o usuário iniciar a remoção com segurança de uma unidade removível durante a criptografia de dados, o Kaspersky Endpoint Security interrompe a criptografia de dados e permite a remoção da unidade removível antes que o processo de criptografia seja concluído.

Se a criptografia de uma unidade removível falhar, visualize o relatório **Criptografia de dados** na interface do Kaspersky Endpoint Security. O acesso a arquivos pode ser bloqueado por outro aplicativo. Neste caso, tente desconectar a unidade removível do computador e conectá-la novamente.

Adicionar uma regra de criptografia para unidades removíveis:

Para adicionar uma regra de criptografia para unidades removíveis:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja adicionar as regras de criptografia de unidade removível.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.

   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de unidades removíveis**.

7. Clique com o botão esquerdo do mouse em **Adicionar** e, na lista suspensa, selecione um dos seguintes itens:

   - Se desejar adicionar regras de criptografia para unidades removíveis que estão na lista de dispositivos confiáveis do componente Controle de Dispositivo, selecione **Da lista de dispositivos confiáveis desta política**.

     A janela **Adicionar dispositivos da lista de dispositivos confiáveis** é exibida.

   - Se desejar adicionar regras de criptografia para unidades removíveis que estão na lista do Kaspersky Security Center, selecione **Da lista de dispositivos do Kaspersky Security Center**.

     A janela **Adicionar dispositivos da lista do Kaspersky Security Center** é exibida.

8. Se tiver selecionado **Da lista de dispositivos do Kaspersky Security Center** na etapa anterior, especifique os filtros para exibir dispositivos na tabela. Para fazer isso:

   a. Especifique os valores dos seguintes parâmetros: **Exibir dispositivos na tabela, para que são configurados os seguintes**, **Tipo do dispositivo**, **Nome**, **Computador** e **Kaspersky Disk Encryption**.

   b. Clique no botão **Atualizar**.

9. Na coluna **Tipo do dispositivo**, marque as caixas de seleção ao lado dos nomes das unidades removíveis para as quais deseja criar regras de criptografia.

10. Na lista suspensa **Modo de criptografia para dispositivos selecionados**, selecione a ação a ser executada pelo Kaspersky Endpoint Security em arquivos armazenados nas unidades removíveis selecionadas.

11. Marque a caixa de seleção **Modo portátil** se desejar que o Kaspersky Endpoint Security prepare as unidades removíveis antes da criptografia, tornando possível usar arquivos criptografados armazenados nessas unidades no modo portátil.

    O modo portátil permite que você utilize arquivos criptografados armazenados nas unidades removíveis que estão conectadas a computadores sem a funcionalidade de criptografia.

12. Marque a caixa de seleção **Criptografar somente espaço usado em disco** se desejar que o Kaspersky Endpoint Security criptografe somente aqueles setores de disco que são ocupados por arquivos.

    Se você estiver aplicando a criptografia em uma unidade que já está em uso, recomenda-se criptografar a unidade inteira. Isto assegura que todos os dados sejam protegidos, até os dados excluídos que ainda podem conter informações recuperáveis. A função **Criptografar somente espaço usado em disco** é recomendada para novas unidades que não foram usadas anteriormente.

    Se um dispositivo tiver sido previamente criptografado usando a função **Criptografar somente espaço usado em disco**, depois de aplicar uma política no modo **Criptografar toda a unidade removível**, os setores que não são ocupados por arquivos ainda não serão criptografados.

13. Na lista suspensa **Ações para dispositivos que foram selecionados anteriormente**, selecione a ação a ser executada pelo Kaspersky Endpoint Security de acordo com as regras de criptografia que foram definidas anteriormente para unidades removíveis.

    - Se desejar que a regra de criptografia anteriormente criada da unidade removível permaneça inalterada, selecione **Ignorar**.

    - Se desejar que uma regra de criptografia criada anteriormente para uma unidade de remoção seja substituída pela nova regra, selecione **Atualização**.

14. Clique em **OK**.

    As linhas contendo parâmetros das regras de criptografia criadas aparecem na tabela **Regras personalizadas**.

15. Clique em **OK** para salvar as alterações.

As regras de criptografia de unidades removíveis adicionadas são aplicadas às unidades removíveis que estão conectadas a quaisquer computadores controlados pela política modificada do Kaspersky Security Center.

Editar uma regra de criptografia para unidades removíveis

Para editar uma regra de criptografia para uma unidade removível:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** na árvore de Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja editar a regra de criptografia da unidade removível.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

    - No menu de contexto da política, selecione **Propriedades**.

    - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de unidades removíveis**.

7. Na lista de unidades removíveis para a qual as regras de criptografia foram configuradas, selecione uma entrada correspondente à unidade removível que você precisa.

8. Clique no botão **Definir uma regra** para editar a regra de criptografia para a unidade removível selecionada.

    O menu de contexto do botão **Definir uma regra** abre.

9. No menu de contexto do botão **Definir uma regra**, selecione a ação a ser executada pelo Kaspersky Endpoint Security em arquivos armazenados na unidade removível selecionada.

10. Clique em **OK** para salvar as alterações.

As regras modificadas de criptografia de unidades removíveis são aplicadas às unidades removíveis que estão conectadas em quaisquer computadores controlados pela política modificada do Kaspersky Security Center.

Ativar o modo portátil para acessar arquivos criptografados em unidades removíveis

Para ativar o modo portátil para acessar arquivos criptografados em unidades removíveis:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual você deseja ativar o modo portátil para acessar arquivos criptografados em unidades removíveis.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de unidades removíveis**.
7. Marque a caixa de seleção **Modo portátil**.

   O modo portátil está disponível apenas para a criptografia de todos os arquivos ou novos arquivos.

8. Clique em **OK**.
9. Aplique a política.

   Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center
10. Conecte a unidade removível a um dispositivo no qual a política do Kaspersky Security Center foi aplicada.
11. Confirme a operação de criptografia de unidade removível.

    Isso abre uma janela na qual você pode criar uma senha do Gerenciador de Arquivos Portátil.
12. Especifique uma senha que atende aos requisitos de força e confirme-o.
13. Clique em **OK**.

    O Kaspersky Endpoint Security criptografa arquivos em uma unidade removível segundo as regras de criptografia definidas na política do Kaspersky Security Center. O Gerenciador de Arquivos Portátil usado para funcionar com arquivos criptografados também será gravado na unidade removível.

Depois de ativar o modo portátil, você pode acessar os arquivos criptografados em unidades removíveis conectadas a um computador sem a funcionalidade de criptografia.

Descriptografia de unidades removíveis

Para descriptografar unidades removíveis:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** na árvore de Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja configurar a descriptografia de unidades removíveis.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de unidades removíveis**.
7. Se desejar descriptografar todos os arquivos criptografados armazenados em unidades removíveis, na lista suspensa **Modo de criptografia**, selecione **Descriptografar toda a unidade removível**.
8. Para descriptografar dados armazenados em unidades removíveis, edite as regras de criptografia para as unidades removíveis cujos dados deseja descriptografar. Para fazer isso:
   a. Na lista de unidades removíveis para a qual as regras de criptografia foram configuradas, selecione uma entrada correspondente à unidade removível que você precisa.
   b. Clique no botão **Definir uma regra** para editar a regra de criptografia para a unidade removível selecionada.
      O menu de contexto do botão **Definir uma regra** abre.
   c. Selecione o item **Descriptografar todos os arquivos** no menu de contexto do botão **Definir uma regra**.
9. Clique em **OK** para salvar as alterações.
10. Aplique a política.

Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Após a aplicação da política, quando o usuário conectar uma unidade removível ou se uma unidade removível já estiver conectada, o Kaspersky Endpoint Security notifica o usuário de que a unidade removível está sujeita à regra de criptografia em que os arquivos criptografados armazenados nesta unidade, bem como seu arquivo de sistema (caso esteja criptografada), serão descriptografados. O aplicativo avisa o usuário que o processo de descriptografia pode demorar algum tempo.

A política do Kaspersky Security Center com configurações predefinidas para criptografia de dados em unidades removíveis é formada por um grupo específico de computadores gerenciados. Portanto, o resultado da descriptografia de dados em unidades removíveis depende do computador em que a unidade removível for conectado.

Se o usuário iniciar a remoção com segurança de uma unidade removível durante a descriptografia de dados, o Kaspersky Endpoint Security interrompe a descriptografia de dados e permite a remoção da unidade removível antes que a operação de descriptografia seja concluída.

Se a descriptografia de uma unidade removível falhar, visualize o relatório **Criptografia de dados** na interface do Kaspersky Endpoint Security. O acesso a arquivos pode ser bloqueado por outro aplicativo. Neste caso, tente desconectar a unidade removível do computador e conectá-la novamente.

Criptografia de discos rígidos

Se o Kaspersky Endpoint Security for instalado em um computador com o Microsoft Windows para Workstations, as tecnologias Criptografia de Unidade de Disco BitLocker e Kaspersky Disk Encryption estão disponíveis para criptografia. Se o Kaspersky Endpoint Security for instalado em um computador com o Microsoft Windows para servidores de arquivo, somente a tecnologia Criptografia de Unidade de Disco BitLocker fica disponível.

Essa seção contém informações sobre a criptografia de discos rígidos e instruções sobre como configurar e realizar a criptografia de discos rígidos com o Kaspersky Endpoint Security e o Plug-in do Console do Kaspersky Endpoint Security.

Sobre a criptografia de discos rígidos

Antes de iniciar a criptografia do disco rígido, o aplicativo executa várias verificações para determinar se o dispositivo pode ser criptografado, incluindo a verificação do disco rígido do sistema quanto à compatibilidade com o Agente de Autenticação e com os componentes de criptografia do BitLocker. Para verificar a compatibilidade, o computador deve ser reiniciado. Após o reinício do computador, o aplicativo executa todas as verificações necessárias automaticamente. Se a verificação de compatibilidade for bem sucedida, a criptografia de disco rígido começa depois que o sistema operacional for inicializado e o aplicativo iniciado. Se o disco rígido do sistema for considerado como incompatível com o Agente de Autenticação ou com os componentes de criptografia do BitLocker, é necessário reinicializar o computador, pressionando o botão de reinício do hardware. O Kaspersky Endpoint Security registra informações sobre a incompatibilidade. Com base nessa informação, o aplicativo não inicia a criptografia de discos rígidos ao iniciar o sistema operacional. As informações sobre este evento são registradas em relatórios do Kaspersky Security Center.

Se a configuração de hardware do computador tiver sido alterada, as informações de incompatibilidade registradas pelo aplicativo durante a verificação anterior devem ser excluídas para verificar a compatibilidade do disco rígido do sistema com o Agente de Autenticação e com os componentes de criptografia do BitLocker. Para isso, antes da criptografia do disco rígido, insira `avp pbatestreset` na linha de comando. Se o sistema operacional não conseguir carregar depois que o disco rígido do sistema tiver sido verificado quanto a compatibilidade com o Agente de Autenticação, você deve remover os objetos e resto de dados depois da operação de teste do Agente de Autenticação usando o Utilitário de Restauração e, em seguida, deve iniciar o Kaspersky Endpoint Security e executar o comando `avp pbatestreset` novamente.

Depois que a criptografia do disco rígido tiver começado, o Kaspersky Endpoint Security criptografa todos os dados gravados em discos rígidos.

Se o usuário desliga ou reinicia o computador durante uma tarefa de descriptografia de disco rígido, o Agente de Autenticação é carregado antes da próxima reinicialização do sistema operacional. O Kaspersky Endpoint Security reinicia a criptografia de discos rígidos após a autenticação com êxito no agente de autenticação e a inicialização do sistema operacional.

Se o sistema operacional alterna para o modo de hibernação durante a criptografia de disco rígido, o Agente de Autenticação é carregado quando o sistema operacional voltar do modo de hibernação. O Kaspersky Endpoint Security reinicia a criptografia de discos rígidos após a autenticação com êxito no agente de autenticação e a inicialização do sistema operacional.

Se o sistema operacional entrar no modo de suspensão durante a criptografia de discos rígidos, o Kaspersky Endpoint Security reinicia a criptografia de discos rígidos quando o sistema operacional acordar da suspensão sem carregar o Agente de Autenticação.

A autenticação do usuário no Agente de Autenticação pode ser realizada de duas formas:

- Insira o nome e a senha da conta do Agente de Autenticação criada pelo administrador de rede local usando as ferramentas do Kaspersky Security Center.
- Insira a senha de um token ou cartão inteligente conectado ao computador.

O agente de autenticação suporta layouts de teclado para os seguintes idiomas:

- Inglês (Reino Unido)
- Inglês (Estados Unidos)
- Árabe (Argélia, Marrocos, Tunísia; layout AZERTY)
- Espanhol (América Latina)
- Italiano
- Alemão (Alemanha e Áustria)
- Alemão (Suíça)
- Português (Brasil, layout ABNT2)
- Russo (para teclados IBM/Windows de 105 teclas com o layout QWERTY)
- Turco (layout QWERTY)
- Francês (França)
- Francês (Suíça)
- Francês (Bélgica, layout AZERTY)
- Japonês (para teclados de 106 teclas com o layout QWERTY)

Um layout de teclado fica disponível no Agente de Autenticação se esse layout tiver sido adicionado às configurações regionais e de idioma do sistema operacional e se tiver ficado disponível na tela de boas-vindas do Microsoft Windows.

Se o nome da conta do Agente de Autenticação contiver símbolos que não possam ser inseridos usando os layouts do teclado disponíveis no Agente de Autenticação, os discos rígidos criptografados poderão ser acessados apenas depois de serem restaurados usando o Utilitário de Restauração ou depois de o nome da conta e a senha do Agente de Autenticação serem restaurados.

O Kaspersky Endpoint Security suporte os seguintes tokens, leitores de cartões inteligentes e cartões inteligentes:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Cartão inteligente)
- SafeNet eToken 4100 72K Java (Cartão inteligente)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (Cartão inteligente)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (Leitor)
- Gemalto IDPrime .NET 511

Criptografia de discos rígidos usando a tecnologia Kaspersky Disk Encryption

Antes de criptografar discos rígidos em um computador, recomendamos que tenha a certeza de que o computador não está infectado. Para fazer assim, inicie a tarefa de Verificação completa ou Verificação de Áreas Críticas. Criptografar o disco rígido de um computador infectado por um rootkit pode acarretar em sua não operabilidade.

Para criptografar discos rígidos que usam a tecnologia de Kaspersky Disk Encryption:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** na árvore de Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja configurar a criptografia de discos rígidos.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de discos rígidos**.

7. Na lista suspensa de **Tecnologia de Criptografia**, selecione a opção **Kaspersky Disk Encryption**.

   A tecnologia de Kaspersky Disk Encryption não pode ser usada se o computador tiver discos rígidos que foram criptografados por BitLocker.

8. Na lista suspensa **Modo de criptografia**, selecione **Criptografar todos os discos rígidos**.

   Se você tiver de excluir alguns discos rígidos da criptografia, crie uma lista de tais discos rígidos.

9. Selecione um dos métodos de criptografia a seguir:

   - Se desejar aplicar a criptografia somente aos setores de disco rígido que são ocupados por arquivos, selecione a caixa de seleção **Criptografar somente espaço usado em disco**.

     Se você estiver aplicando a criptografia em uma unidade que já está em uso, recomenda-se criptografar a unidade inteira. Isto assegura que todos os dados sejam protegidos, até os dados excluídos que ainda podem conter informações recuperáveis. A função **Criptografar somente espaço usado em disco** é recomendada para novas unidades que não foram usadas anteriormente.

   - Se desejar aplicar a criptografia ao disco rígido inteiro, desmarque a caixa de seleção **Criptografar somente espaço usado em disco**.

     Esta função é aplicável somente a dispositivos não criptografados. Se um dispositivo tiver sido previamente criptografado usando a função **Criptografar somente espaço usado em disco**, depois de aplicar uma política no modo **Criptografar todos os discos rígidos**, os setores que não são ocupados por arquivos ainda não serão criptografados.

10. Clique em **OK** para salvar as alterações.

11. Aplique a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Criptografia de discos rígidos usando a tecnologia Criptografia de Unidade de Disco BitLocker

Antes de criptografar discos rígidos em um computador, recomendamos que tenha a certeza de que o computador não está infectado. Para fazer assim, inicie a tarefa de Verificação completa ou Verificação de Áreas Críticas. Criptografar o disco rígido de um computador infectado por um rootkit pode acarretar em sua não operabilidade.

O uso da tecnologia Criptografia de Unidade de Disco BitLocker em computadores com um sistema operacional de servidor pode necessitar da instalação do componente **Criptografia de Unidade de Disco BitLocker** usando o assistente Adicionar funções e componentes.

Para criptografar discos rígidos usando a tecnologia de Criptografia de Unidade de Disco BitLocker:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** na árvore de Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja configurar a criptografia de discos rígidos.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de discos rígidos**.
7. Na lista suspensa **Tecnologia de Criptografia**, selecione a opção **Criptografia de Unidade de Disco BitLocker**.
8. Na lista suspensa **Modo de criptografia**, selecione a opção **Criptografar todos os discos rígidos**.
9. Se desejar usar um teclado de tela tátil para inserir informações em um ambiente de pré-inicialização, selecione a caixa de seleção **Permitir uso de autenticação que requer entrada do teclado de pré-inicialização nos tablets**.

   Recomenda-se usar esta definição somente para dispositivos que têm ferramentas de entrada de dados alternativas, como um teclado USB em um ambiente de pré-inicialização.

10. Selecione um dos seguintes tipos de criptografia:
    - Se desejar usar a criptografia de hardware, marque a caixa de seleção **Usar criptografia de hardware**.
    - Se desejar usar a criptografia de software, desmarque a caixa de seleção **Usar criptografia de hardware**.

11. Selecione um dos métodos de criptografia a seguir:

    - Se desejar aplicar a criptografia somente aos setores de disco rígido que são ocupados por arquivos, selecione a caixa de seleção **Criptografar somente espaço usado em disco**.
    - Se desejar aplicar a criptografia ao disco rígido inteiro, desmarque a caixa de seleção **Criptografar somente espaço usado em disco**.

    Esta função é aplicável somente a dispositivos não criptografados. Se um dispositivo tiver sido previamente criptografado usando a função **Criptografar somente espaço usado em disco**, depois de aplicar uma política no modo **Criptografar todos os discos rígidos**, os setores que não são ocupados por arquivos ainda não serão criptografados.

12. Selecione um método para acessar discos rígidos que foram criptografados com o BitLocker.

    - Se desejar usar Trusted Platform Module (TPM) para guardar chaves de criptografia, selecione a opção **Usar Trusted Platform Module (TPM)**.
    - Se não estiver usando o Trusted Platform Module (TPM) para a criptografia de discos rígidos, selecione a opção **Usar senha** e especifique o número mínimo de caracteres que uma senha deve conter no campo **Comprimento mínimo da senha**.

    A disponibilidade de um Trusted Platform Module (TPM) é obrigatória para o Windows 7 e sistemas operacionais do Windows 2008 R2, bem como para versões anteriores.

13. Se você tiver selecionado a opção **Usar Trusted Platform Module (TPM)** na etapa anterior:

    - Se desejar definir um código PIN que será solicitado quando o usuário tentar acessar uma chave de criptografia, marque a caixa de seleção **Usar PIN** e, no campo **Comprimento mínimo do PIN**, especifique o número mínimo de dígitos que um código PIN deve conter.
    - Se você gostaria de acessar discos rígidos criptografados sem um módulo de plataforma confiável no computador usando uma senha, marque a caixa de seleção **Usar senha, se Trusted Platform Module (TPM) estiver indisponível** e no campo **Comprimento mínimo da senha**, indique o número mínimo de caracteres que a senha deve conter.

      Neste evento, o acesso a chaves de criptografia ocorrerá usando a senha dada como se a caixa de seleção **Usar senha** for marcada.

    Se a caixa de seleção **Usar senha, se Trusted Platform Module (TPM) estiver indisponível** não estiver marcada e o Trusted Platform Module não estiver disponível, a criptografia do disco rígido não será iniciada.

14. Clique em **OK** para salvar as alterações.

15. Aplique a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Depois de aplicar a política do computador cliente com o Kaspersky Endpoint Security instalado, as seguintes perguntas serão feitas:

- Se a política de criptografia for aplicada a um disco rígido do sistema, a janela de código PIN aparecerá se o módulo de plataforma confiável estiver em uso ou a janela de solicitação de senha aparecerá para a autorização de pré-carregamento.

- Se o sistema operacional do computador tiver o modo Processamento de Informações Federais ativado, o sistema operacional, no Windows 8 ou mais recente, exibirá uma janela de solicitação de conexão de dispositivo USB para salvar o arquivo de chave de recuperação.

Se não houver acesso a chaves de criptografia, o usuário pode solicitar que o administrador de rede local forneça uma chave de recuperação (caso a chave de recuperação não tenha sido salva antes no dispositivo USB ou tiver sido perdida).

Criar uma lista de discos rígidos excluídos da criptografia

Você pode criar uma lista de exclusões da criptografia apenas da tecnologia do Kaspersky Disk Encryption.

Para formar uma lista de discos rígidos excluídos da criptografia:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração em que deseja criar uma lista de discos rígidos a serem excluídos da criptografia.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de discos rígidos**.
7. Na lista suspensa de **Tecnologia de Criptografia**, selecione a opção **Kaspersky Disk Encryption**.

   Entradas correspondentes a discos rígidos excluídos da criptografia aparecem na tabela **Não criptografar os seguintes discos rígidos**. Esta tabela está vazia caso você não tenha formado anteriormente uma lista de discos rígidos a serem excluídos da criptografia.
8. Para adicionar discos rígidos à lista de discos rígidos excluídos da criptografia:
   a. Clique no botão **Adicionar**.

      A janela **Adicionar dispositivos da lista do Kaspersky Security Center** é exibida.
   b. Na janela **Adicionar dispositivos da lista do Kaspersky Security Center**, especifique os valores dos seguintes parâmetros: **Nome**, **Computador**, **Tipo de disco** e **Kaspersky Disk Encryption**.
   c. Clique no botão **Atualizar**.
   d. Na coluna **Nome**, marque as caixas de seleção nas linhas da tabela que correspondem aos discos rígidos que você deseja adicionar à lista de discos rígidos excluídos da criptografia.

e. Clique em **OK**.

Os discos rígidos selecionados aparecem na tabela **Não criptografar os seguintes discos rígidos**.

9. Se desejar remover discos rígidos da tabela de exclusões, selecione uma ou várias linhas na tabela **Não criptografar os seguintes discos rígidos** e clique no botão **Excluir**.

> Para selecionar diversas linhas na tabela, selecione-as pressionando a tecla **CTRL**.

10. Clique em **OK** para salvar as alterações.

Descriptografia de disco rígido

> Você pode descriptografar discos rígidos mesmo se não houver uma licença ativa que permita a criptografia de dados.

Para descriptografar discos rígidos:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore de Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja configurar a descriptografia de discos rígidos.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Criptografia de dados**, selecione a subseção **Criptografia de discos rígidos**.
7. Na lista suspensa **Tecnologia de criptografia**, selecione a tecnologia com a qual os discos rígidos foram criptografados.
8. Execute uma das seguintes ações:
   - Na lista suspensa **Modo de criptografia**, selecione a opção **Descriptografar todos os discos rígidos** para descriptografar todos os discos rígidos criptografados.
   - Adicione os discos rígidos criptografados que você deseja descriptografar para a tabela **Não criptografar os seguintes discos rígidos**.

     > Esta opção está disponível apenas para a tecnologia do Kaspersky Disk Encryption.

9. Clique em **OK** para salvar as alterações.

10. Aplique a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Se o usuário encerrar ou reiniciar o computador durante a descriptografia de discos rígidos que foram criptografados usando a tecnologia do Kaspersky Disk Encryption, o Agente de Autenticação é carregado antes da próxima reinicialização do sistema operacional. O Kaspersky Endpoint Security continua a descriptografia de disco rígido depois da autenticação com êxito no agente de autenticação e da inicialização do sistema operacional.

Se o sistema operacional alternar para o modo de hibernação durante a criptografia de discos rígidos que foram criptografados com a tecnologia do Kaspersky Disk Encryption, o Agente de Autenticação é carregado quando o sistema operacional voltar do modo de hibernação. O Kaspersky Endpoint Security continua a descriptografia de disco rígido depois da autenticação com êxito no agente de autenticação e da inicialização do sistema operacional. Após a descriptografia do disco rígido, o modo de hibernação fica indisponível até que o sistema operacional seja reiniciado da próxima vez.

Se o sistema operacional entrar no modo de suspensão durante a descriptografia do disco rígido, o Kaspersky Endpoint Security reinicia a descriptografia quando o sistema operacional sair do modo de suspensão sem carregar o Agente de Autenticação.

Gerenciar o Agente de Autenticação

Se os discos rígidos do sistema forem criptografados, o Agente de Autenticação é carregado antes da inicialização do sistema operacional. Use o Agente de Autenticação para concluir a autenticação a fim de obter acesso aos discos rígidos do sistema criptografado e carregar o sistema operacional.

Depois de conclusão bem sucedida do procedimento de autenticação, o sistema operacional é carregado. O processo de autenticação é repetido toda vez que o sistema operacional for reiniciado.

O usuário pode não conseguir passar pela autenticação em alguns casos. Por exemplo, a autenticação não será possível se o usuário tiver esquecido as credencias de conta da conta do Agente de Autenticação ou a senha para o token ou cartão inteligente ou se tiver perdido o token ou cartão inteligente.

Se o usuário esqueceu as credenciais da conta do Agente de Autenticação ou a senha de um token ou de um cartão inteligente, você deverá entrar em contato com o administrador da rede local corporativa para recuperá-los.

Se um usuário perdeu um token ou um cartão inteligente, o administrador deverá adicionar o arquivo de um certificado eletrônico do token ou do cartão inteligente ao comando para criar uma conta do Agente de Autenticação. Em seguida, o usuário deve concluir o procedimento para restaurar dados sobre dispositivos criptografados.

Usar um token ou cartão inteligente com o Agente de Autenticação

É possível usar um token ou cartão inteligente para a autenticação quando acessar discos rígidos criptografados. Para isso, você deve adicionar o arquivo de um certificado eletrônico do token ou cartão inteligente ao comando para criar uma conta do Agente de Autenticação.

O uso de um token ou cartão inteligente estará disponível somente se os discos rígidos do computador tiverem sido criptografados usando o algoritmo de criptografia AES256. Se os discos rígidos do computador foram criptografados usando o algoritmo de criptografia AES56, a adição do arquivo de certificado eletrônico ao comando será negada.

Para adicionar o arquivo de certificado eletrônico de um token ou cartão inteligente ao comando para criar uma conta do Agente de Autenticação, primeiro salve o arquivo usando software de terceiros para gerenciar certificados.

O certificado do token ou cartão inteligente tem as seguintes propriedades:

- O certificado deve ser compatível com a norma X.509 e o arquivo do certificado deve ter a codificação DER.

  Se o certificado eletrônico do token ou cartão inteligente não atender a esse requisito, o plug-in de administração não carregará o arquivo desse certificado para o comando para criar uma conta do Agente de Autenticação e exibirá uma mensagem de erro.

- O parâmetro `KeyUsage` que define a finalidade do certificado deve ter o valor `keyEncipherment` ou `dataEncipherment`.

  Se o certificado eletrônico do token ou cartão inteligente não atender a esse requisito, o plug-in carregará o arquivo desse certificado para o comando para criar uma conta do Agente de Autenticação e exibirá uma mensagem de advertência.

- O certificado contém uma chave RSA com um comprimento de pelo menos 1.024 bits.

  Se o certificado eletrônico do token ou cartão inteligente não atender a esse requisito, o plug-in de administração não carregará o arquivo desse certificado para o comando para criar uma conta do Agente de Autenticação e exibirá uma mensagem de erro.

Editar as mensagens de ajuda do Agente de Autenticação

Antes de editar mensagens de ajuda do Agente de Autenticação, por favor reveja a lista de caracteres suportados em um ambiente de pré-reinicialização.

Para editar as mensagens de ajuda do Agente de Autenticação:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja editar as mensagens de ajuda do Agente de Autenticação.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Criptografia de dados**, selecione a subseção **Configurações comuns de criptografia**.

7. Na seção **Modelos**, clique no botão **Ajuda**.

   É exibida a janela **Mensagens de ajuda do Agente de Autenticação**.

8. Faça o seguinte:

   - Selecione a guia **Autenticação** para editar o texto de ajuda mostrado na janela do Agente de Autenticação quando as credenciais de conta estão sendo inseridas.
   - Selecione a guia **Alterar senha** para editar o texto de ajuda exibido na janela do Agente de Autenticação quando a senha para a conta do Agente de Autenticação estiver sendo alterada.
   - Selecione a guia **Recuperar senha** para editar o texto de ajuda exibido na janela do Agente de Autenticação quando a senha da conta do Agente de Autenticação estiver sendo recuperada.

9. Edite as mensagens de ajuda.

   Se desejar restaurar o texto original, clique no botão **Padrão**.

10. Clique em **OK**.

11. Para salvar as alterações, na janela **Propriedades: <Nome de política>**, clique em **OK**.

O suporte limitado de caracteres nas mensagens de ajuda do Agente de Autenticação

Em um ambiente de pré-reinicialização, os seguintes caracteres Unicode são suportados:

- Alfabeto latino básico (0000 – 007F)
- Caracteres adicionais Latim 1 (0080 – 00FF)
- Latim-A estendido (0100 – 017F)
- Latim-B extenso (0180 – 024F)
- Caracteres de ID estendidos não combinados (02B0 – 02FF)
- Marcas diacríticas combinadas (0300 – 036F)
- Alfabetos gregos e coptos (0370 – 03FF)
- Cirílico (0400 – 04FF)
- Hebraico (0590 – 05FF)
- Script arábico (0600 – 06FF)
- Latim estendido adicional (1E00 – 1EFF)
- Marcas de pontuação (2000 – 206F)
- Símbolos de moeda (20A0 – 20CF)

- Símbolos parecidos com letras (2100 – 214F)
- Números geométricos (25A0 – 25FF)
- Formulários de apresentação de script-B arábico (FE70 – FEFF)

Os caracteres que não são especificados nesta lista não são apoiados em um meio de pré-inicialização. Não se recomenda usar tais caracteres em mensagens de ajuda do Agente de Autenticação.

Selecionar o nível de rastreio do Agente de Autenticação

O aplicativo registra informações de serviço sobre a operação do Agente de Autenticação e informações sobre as operações do usuário com o Agente de Autenticação no arquivo de rastreio. O arquivo de rastreio do Agente de Autenticação pode ser muito útil se você precisar de restaurar dados em discos rígidos criptografados.

Para selecionar o nível de rastreio do Agente de Autenticação:

1. Logo que um computador com discos rígidos criptografados é inicializado, pressione o botão **F3** para abrir uma janela e especificar as configurações do Agente de Autenticação.
2. Selecione o nível de rastreio na janela de configurações do Agente de Autenticação:
   - **Desativar o registo de depuração (padrão)**. Se esta opção for marcada, o aplicativo não registra informações sobre eventos do Agente de Autenticação no arquivo de rastreio.
   - **Ativar o registo de depuração**. Se essa opção for marcada, o aplicativo registra informações sobre a operação do Agente de Autenticação e as operações do usuário realizadas com o Agente de Autenticação no arquivo de rastreio.
   - **Ativar registo detalhado**. Se essa opção for marcada, o aplicativo registra no arquivo de rastreio informações sobre a operação do Agente de Autenticação e as operações do usuário realizadas com o Agente de Autenticação.

     O nível de detalhe das entradas nessa opção é mais elevado comparado ao nível da opção **Ativar o registro de depuração**. Um nível elevado de detalhe das entradas pode retardar a inicialização do Agente de Autenticação e do sistema operacional.

   - **Ativar registo de depuração e selecionar porta serial**. Se essa opção for marcada, o aplicativo registra no arquivo de rastreio informações sobre a operação do Agente de Autenticação e as operações do usuário realizadas com o Agente de Autenticação, depois as transmite via porta COM.

     Se um computador com unidades de disco rígido criptografada for conectado a outro computador via porta COM, os eventos do Agente de Autenticação podem ser examinados por esse outro computador.

   - **Ativar registro detalhado de depuração e selecionar porta serial**. Se essa opção for marcada, o aplicativo registra no arquivo de rastreio informações detalhadas sobre a operação do Agente de Autenticação e as operações do usuário realizadas com o Agente de Autenticação, depois as transmite via porta COM.

O nível de detalhe das entradas nessa opção é mais elevado comparado ao nível da opção **Ativar o registro de depuração e selecionar a porta serial**. Um nível elevado de detalhe das entradas pode retardar a inicialização do Agente de Autenticação e do sistema operacional.

Os dados são registrados no arquivo de rastreio do Agente de Autenticação se existirem discos rígidos criptografados no computador ou durante a criptografia de discos rígidos.

O arquivo de rastreio do Agente de Autenticação não é enviado à Kaspersky, diferentemente dos outros arquivos de rastreio do aplicativo. Se necessário, o administrador do sistema pode enviar manualmente o arquivo de rastreio do Agente de Autenticação para a Kaspersky, para análise.

Gerenciar contas do Agente de Autenticação

As ferramentas do Kaspersky Security Center a seguir estão disponíveis para o gerenciamento de contas do Agente de Autenticação:

- Tarefa de grupo para gerenciar contas do Agente de Autenticação. Esta tarefa permite que você gerencie contas do Agente de Autenticação para um grupo de computadores clientes.
- Tarefa local de **Criptografia (gerenciamento de contas)**. Esta tarefa permite que você gerencia contas do Agente de Autenticação para computadores clientes individuais.

Para definir as configurações da tarefa de gerenciamento de contas do Agente de Autenticação:

1. Crie (Criar uma tarefa local, Criar uma tarefa de grupo) uma tarefa de gereciamento de contas do Agente de Autenticação.
2. Abra a seção **Configurações** na janela **Propriedades: <Nome da tarefa de gerenciamento de conta do Agente de Autenticação>**.
3. Adicione comandos para criar contas do Agente de Autenticação.
4. Adicione comandos para editar contas do Agente de Autenticação.
5. Adicione comandos para excluir contas do Agente de Autenticação do usuário.
6. Se necessário, edite os comandos adicionados para gerenciar as contas do Agente de Autenticação. Para isso, selecione um comando na tabela **Comandos para gerenciar contas do Agente de Autenticação** e clique no botão **Editar**.
7. Se necessário, exclua os comandos adicionados para gerenciar as contas do Agente de Autenticação. Para isso, selecione um ou vários comandos na tabela **Comandos para gerenciar contas do Agente de Autenticação** e clique no botão **Remover**.

   Para selecionar diversas linhas na tabela, selecione-as pressionando a tecla **CTRL**.

8. Para salvar as modificações, clique em **OK** na janela de propriedades de tarefa.
9. Execute a tarefa.

Os comandos do gerenciamento de contas do Agente de Autenticação adicionados à tarefa são executados.

Adicionar um comando para criar uma conta do Agente de Autenticação

Para adicionar um comando para criar uma conta do Agente de Autenticação:

1. Abra a seção **Configurações** na janela **Propriedades: <Nome da tarefa de gerenciamento de conta do Agente de Autenticação>**.

2. Clicar no botão **Adicionar** e na lista suspensa selecione o **Comando de adição de conta**.

   A janela **Adicionar conta de usuário** abre.

3. No campo **Adicionar conta de usuário** na janela **Conta do Windows**, especifique o nome da conta do Microsoft Windows com base em qual conta do Agente de Autenticação será criada.

   Para isso, digite o nome da conta manualmente ou clique no botão **Selecionar**.

4. Se você inseriu o nome de uma conta de usuário do Microsoft Windows manualmente, clique no botão **Permitir** para determinar o identificador de segurança (SID) da conta.

   Se você escolher não determinar o identificador de segurança (SID) clicando no botão **Permitir**, o SID será determinado no momento em que a tarefa for executada no computador.

   > Determinar o SID da conta de usuário do Microsoft Windows ao adicionar o comando de criação da conta do Agente de Autenticação é uma maneira conveniente de garantir que a conta de usuário do Microsoft Windows inserida manualmente esteja correta. Se a conta de usuário do Microsoft Windows inserida não existir, ela pertence a um domínio não confiável, ou não existe no computador para o qual a tarefa local **Criptografia (gerenciamento de conta)** está sendo modificada, a tarefa de gerenciamento da conta do Agente de Autenticação termina com um erro.

5. Marque a caixa de seleção **Alterar conta de usuário existente** para ter uma conta com um nome idêntico à criada anteriormente para o Agente de Autenticação, que será substituída pela nova conta.

   > Esta etapa está disponível quando você adicionar o comando de criação de conta do Agente de Autenticação nas propriedades de uma tarefa de grupo para gerenciar contas do Agente de Autenticação. Esta etapa não estará disponível se você estiver adicionando o comando de criação de conta do Agente de Autenticação nas propriedades de uma tarefa local de **Criptografia (gerenciamento de contas)**.

6. No campo **Nome de usuário**, digite o nome da conta do Agente de Autenticação que deve ser inserido durante o processo de autenticação para acessar os discos rígidos criptografados.

7. Marque a caixa de seleção **Permitir autenticação baseada em senha** se desejar que o aplicativo solicite a inserção da senha da conta do Agente de Autenticação durante o processo de autenticação para acessar os discos rígidos criptografados.

8. Se você tiver marcado a caixa de seleção **Permitir autenticação baseada em senha** na etapa anterior:

   a. No campo **Senha**, digite a senha da conta do Agente de Autenticação que deve ser inserida durante o processo de autenticação para acessar os discos rígidos criptografados.

   b. No campo **Confirmar senha**, confirme a senha da conta do Agente de Autenticação inserida na etapa anterior.

   c. Execute uma das seguintes ações:

- Marque a opção **Alterar senha na primeira autenticação** se desejar que o aplicativo exiba uma solicitação de alteração de senha ao usuário que passar pela autenticação com a conta especificada no comando pela primeira vez.

- Caso contrário, selecione a opção **Não solicitar alteração de senha**.

9. Marque a caixa de seleção **Permitir autenticação baseada em certificado** se desejar que o aplicativo solicite que o usuário conecte um token ou cartão inteligente ao computador durante o processo de autenticação, para acessar os discos rígidos criptografados.

10. Se você tiver marcado a caixa de seleção **Permitir autenticação baseada em certificado** na etapa anterior, clique no botão **Procurar** e selecione o arquivo do certificado eletrônico do token ou cartão inteligente na janela **Selecionar arquivo de certificado**.

11. Se necessário, no campo **Descrição do comando**, insira os detalhes da conta do Agente de Autenticação que você precisa para gerenciar o comando.

12. Execute uma das seguintes ações:

    - Marque a caixa de seleção **Permitir autenticação** se desejar que o aplicativo permita que o usuário que estiver utilizando a conta especificada no comando acesse o diálogo de autenticação no Agente de Autenticação.

    - Marque a caixa de seleção **Bloquear autenticação** se desejar que o aplicativo impeça que o usuário que estiver utilizando a conta especificada no comando acesse o diálogo de autenticação no Agente de Autenticação.

13. Na janela **Adicionar conta de usuário**, clique em **OK**.

Adicionar um comando de edição de conta do Agente de Autenticação

Para adicionar um comando para editar uma conta do Agente de Autenticação:

1. Na seção **Configurações** das **Propriedades: <nome da tarefa de gerenciamento de conta do Agente de Autenticação>**, abra o menu de contexto do botão **Adicionar** e selecione o item **Comando de edição de conta**.

   A janela **Editar conta de usuário** abre.

2. No campo **Conta do Windows** na janela **Editar conta de usuário**, especifique o nome da conta de usuário do Microsoft Windows que foi usada para criar a conta do Agente de Autenticação que você deseja editar. Para isso, digite o nome da conta manualmente ou clique no botão **Selecionar**.

3. Se você inseriu o nome de uma conta de usuário do Microsoft Windows manualmente, clique no botão **Permitir** para determinar o identificador de segurança (SID) da conta do usuário.

   Se você escolher não determinar o identificador de segurança (SID) clicando no botão **Permitir**, o SID será determinado no momento em que a tarefa for executada no computador.

   Determinar o SID da conta de usuário do Microsoft Windows ao adicionar o comando de edição da conta do Agente de Autenticação é uma maneira conveniente de garantir que a conta de usuário do Microsoft Windows inserida manualmente esteja correta. Se a conta de usuário do Microsoft Windows inserida não existir ou pertencer a um domínio não confiável, a tarefa de gerenciamento da conta do Agente de Autenticação termina com um erro.

4. Marque a caixa de seleção **Alterar nome do usuário** e insira um novo nome para a conta do Agente de Autenticação se desejar que o Kaspersky Endpoint Security altere o nome de usuário de todas as contas do Agente de Autenticação criadas com base na conta do Microsoft Windows com o nome indicado no campo **Conta do Windows** para o nome inserido no campo abaixo.

5. Marque a caixa de seleção **Modificar configurações de autenticação baseadas em senha** para tornar editáveis as configurações de autenticação baseada em senha.

6. Marque a caixa de seleção **Permitir autenticação baseada em senha** se desejar que o aplicativo solicite a inserção da senha da conta do Agente de Autenticação durante o processo de autenticação para acessar os discos rígidos criptografados.

7. Se você tiver marcado a caixa de seleção **Permitir autenticação baseada em senha** na etapa anterior:

   a. No campo **Senha**, insira a nova senha da conta do Agente de Autenticação.

   b. No campo **Confirmar senha**, confirme a senha inserida na etapa anterior.

8. Marque a caixa de seleção **Editar a regra de alteração de senha na autenticação do Agente de Autenticação** se desejar que o Kaspersky Endpoint Security altere o valor da configuração de alteração de senha para todas as contas do Agente de Autenticação criadas usando a conta do Microsoft Windows com o nome indicado no campo **conta do Windows** para o valor de configuração especificado abaixo.

9. Especifique o valor da configuração de alteração da senha na autenticação do Agente de Autenticação.

10. Marque a caixa de seleção **Modificar configurações de autenticação baseadas em certificado** para tornar editáveis as configurações da autenticação baseadas no certificado eletrônico de um token ou cartão inteligente.

11. Marque a caixa de seleção **Permitir autenticação baseada em certificado** se desejar que o aplicativo solicite que o usuário insira a senha para o token ou cartão inteligente conectado ao computador durante o processo de autenticação, para poder acessar os discos rígidos criptografados.

12. Se você tiver marcado a caixa de seleção **Permitir autenticação baseada em certificado** na etapa anterior, clique no botão **Procurar** e selecione o arquivo do certificado eletrônico do token ou cartão inteligente na janela **Selecionar arquivo de certificado**.

13. Marque a caixa de seleção **Editar descrição de comando** e edite a descrição do comando se desejar que o Kaspersky Endpoint Security altere a descrição do comando para todas as contas do Agente de Autenticação criadas com base nas contas do Microsoft Windows com o nome indicado no campo **Conta do Windows**.

14. Marque a caixa de seleção **Editar a regra de acesso à autenticação no Agente de Autenticação** se você desejar que o Kaspersky Endpoint Security altere a regra de acesso do usuário do diálogo de autenticação no Agente de Autenticação para o valor especificado abaixo para todas as contas do Agente de Autenticação criadas usando a conta do Microsoft Windows com o nome indicado no campo **Conta do Windows**.

15. Especifique a regra para acessar a caixa de diálogo de autenticação no Agente de Autenticação.

16. Na janela **Editar conta de usuário**, clique em **OK**.

Adicionar um comando para excluir uma conta do Agente de Autenticação

Para adicionar um comando para excluir uma conta do Agente de Autenticação:

1. Na seção **Configurações** da janela **Propriedades: <nome da tarefa de gerenciamento de conta do Agente de Autenticação>**, abra o menu de contexto do botão **Adicionar** e selecione o **Comando de exclusão de conta**.

   A janela **Excluir conta do usuário** abre.

2. No campo **Conta do Windows** na janela **Excluir conta do usuário**, especifique o nome da conta de usuário do Microsoft Windows que foi usada para criar a conta do Agente de Autenticação que você deseja excluir. Para isso, digite o nome da conta manualmente ou clique no botão **Selecionar**.

3. Se você inseriu o nome de uma conta de usuário do Microsoft Windows manualmente, clique no botão **Permitir** para determinar o identificador de segurança (SID) da conta do usuário.

   Se você escolher não determinar o identificador de segurança (SID) clicando no botão **Permitir**, o SID será determinado no momento em que a tarefa for executada no computador.

   > Determinar o SID da conta de usuário do Microsoft Windows quando adicionar o comando de exclusão de conta do Agente de Autenticação é uma maneira conveniente de garantir que a conta de usuário do Microsoft Windows inserida manualmente esteja correta. Se a conta de usuário do Microsoft Windows inserida não existir ou pertencer a um domínio não confiável, a tarefa de gerenciamento da conta do Agente de Autenticação termina com um erro.

4. Na janela **Excluir conta do usuário**, clique em **OK**.

Restaurar credenciais da conta do Agente de Autenticação

> Estas instruções são destinadas para usuários de computadores de cliente com Kaspersky Endpoint Security instalado.

Para restaurar o nome de usuário e a senha de uma conta do Agente de Autenticação:

1. O Agente de Autenticação é carregado em um computador com discos rígidos criptografados antes que o sistema operacional seja carregado. Na interface do Agente de Autenticação, clique no botão **Esqueci a senha** para iniciar o processo de restauração do nome de usuário e da senha de uma conta do Agente de Autenticação.

2. Siga as instruções do Agente de Autenticação para obter as unidades necessárias para restaurar o nome de usuário e a senha da conta do Agente de Autenticação.

3. Declare o conteúdo dos bloqueios de solicitação para o administrador de rede local da sua empresa junto com o nome do computador.

4. Insira as seções da resposta da solicitação de restauração de nome de usuário e senha da conta do Agente de Autenticação e que foram geradas e fornecidas pelo administrador da rede local.

5. Insira uma nova senha para a conta do Agente de Autenticação e confirme-a.

   O nome de usuário da conta do Agente de Autenticação é definido utilizando as seções de resposta às solicitações de restauração do nome de usuário e da senha da conta do Agente de Autenticação.

Depois de inserir e confirma a nova senha da conta do Agente de Autenticação, a senha será salva e você terá acesso aos discos rígidos criptografados.

Responder a uma solicitação de usuário para restaurar credenciais de conta do Agente de Autenticação

Para criar e enviar as seções de usuário da resposta à solicitação de restauração do nome de usuário e senha de uma conta do Agente de Autenticação:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração que inclui o computador do usuário que solicitou a restauração do nome de usuário e senha de uma conta do Agente de Autenticação.
3. No espaço de trabalho, selecione a guia **Dispositivos**.
4. Na guia **Dispositivos**, selecione o computador do usuário que solicitou a restauração do nome de usuário e senha de uma conta do Agente de Autenticação e clique com o botão direito para abrir o menu de contexto.
5. No menu de contexto, selecione a opção **Conceder acesso a dispositivos e dados em modo off-line**.

   A janela **Conceder acesso a dispositivos e dados em modo off-line** é exibida.
6. Na janela **Conceder acesso a dispositivos e dados em modo off-line**, selecione a guia **Agente de Autenticação**.
7. Na seção **Algoritmo de criptografia em uso**, selecione o tipo do algoritmo de criptografia.
8. Na lista suspensa **Conta**, selecione o nome da conta do Agente de Autenticação criada para o usuário que solicitou a recuperação do nome e senha da conta do Agente de Autenticação.
9. Na lista suspensa **Disco rígido**, selecione o disco rígido criptografado para o qual você precisa recuperar o acesso.
10. Na seção **Solicitação do usuário**, insira os blocos da solicitação declarada pelo usuário.

    O conteúdo das seções da resposta à solicitação do usuário para recuperação do nome de usuário e senha de uma conta do Agente de Autenticação será exibido no campo **Chave de acesso**.
11. Declare os conteúdos dos blocos de resposta ao usuário.

Exibir os detalhes da criptografia de dados

Esta seção descreve como exibir os detalhes da criptografia de dados.

Sobre o status da criptografia

Enquanto a criptografia ou a descriptografia estão em andamento, o Kaspersky Endpoint Security retransmite informações do status dos parâmetros de criptografia aplicadas aos computadores clientes para o Kaspersky Security Center.

São possíveis os seguintes valores de status da criptografia:

- *Política indefinida*. Uma política do Kaspersky Security Center que não foi definida para o computador.
- *Criptografia/descriptografia em andamento*. A criptografia e/ou descriptografia de dados está em andamento no computador.
- *Erro*. Ocorreu um erro durante a criptografia e/ou descriptografia dos dados no computador.
- *Reinício necessário*. O sistema operacional tem que ser reiniciado para iniciar ou terminar a criptografia ou descriptografia dos dados do computador.
- *Conforme a política*. A criptografia e/ou descriptografia no computador foi concluída usando as configurações de criptografia especificadas na política do Kaspersky Security Center aplicada ao computador.
- *Cancelado pelo usuário*. O usuário recusou confirmar a operação de criptografia do arquivo na unidade removível.
- *Sem suporte*. A funcionalidade de criptografia está indisponível no computador.

Exibir o status da criptografia

Para visualizar o status da criptografia dos dados do computador:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertence o computador desejado.
3. No espaço de trabalho, selecione a guia **Dispositivos**.

   A guia **Dispositivos** na área de trabalho exibe propriedades dos computadores no grupo de administração selecionado.
4. Na guia **Dispositivos** na área de trabalho, deslize a barra de rolagem completamente à direita.

   A coluna **Status da criptografia** exibe os status da criptografia dos dados nos computadores no grupo de administração selecionado. Esse status é formado com base nas informações sobre a criptografia de arquivo em unidades locais do computador, a criptografia de discos rígidos do computador e a criptografia de unidades removíveis conectadas ao computador.

Exibir o status da criptografia nos painéis de detalhes do Kaspersky Security Center

Para visualizar o status da criptografia nos painéis de detalhes do Kaspersky Security Center:

1. Abra o Console de Administração do Kaspersky Security Center.
2. No árvore do console, selecione o nó **Servidor de administração – <Nome de computador>**.
3. Na área de trabalho à direita da árvore do Console de Administração, selecione a guia **Estatísticas**.

4. Crie uma nova página com painéis de detalhes com estatísticas de criptografia de dados. Para fazer isso:

   a. Na guia **Estatísticas**, clique no botão **Personalizar exibição**.

      A janela **Propriedades: Estatísticas** abre.

   b. Na janela **Propriedades: Estatísticas**, clique em **Adicionar**.

      A janela **Propriedades: Nova página** abre.

   c. Na seção **Geral** da janela **Propriedades: Nova página**, digite o nome da página.

   d. Na seção **Painéis de detalhes**, clique no botão **Adicionar**.

      A janela **Novo painel de detalhes** abre.

   e. Na janela **Novo painel de detalhes** no grupo **Status de Proteção**, selecione o item de **Criptografia do dispositivo**.

   f. Clique em **OK**.

      A janela **Propriedades: Controle de Criptografia** é exibida.

   g. Se necessário, edite as configurações do painel de detalhes. Para isso, use as seções **Exibir** e **Dispositivos** da janela **Propriedades: Criptografia do dispositivo**.

   h. Clique em **OK**.

   i. Repita os passos d – h das instruções, selecionando o item **Criptografia de unidades removíveis** na seção **Status de proteção** da janela **Novo painel de detalhes**.

      Os painéis de detalhes adicionados aparecem nas listas **Painéis de detalhes** na janela **Propriedades: Nova página**.

   j. Na janela **Propriedades: Nova página**, clique em **OK**.

      O nome da página com painéis de detalhes criados nos passos anteriores aparecem na lista **Páginas** da janela **Propriedades: Estatísticas**.

   k. Na janela **Propriedades: Estatísticas**, clique em **Fechar**.

5. Na guia **Estatísticas** , abra a página criada nas etapas anteriores das instruções.

O painel de detalhes aparece, mostrando o status da criptografia dos computadores e unidades removíveis.

Exibir erros de criptografia de arquivos em unidades de computador locais

Para exibir os erros de criptografia de arquivo em unidades de computador locais:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** da árvore do console Administração, abra a pasta com o nome do grupo de administração que inclui o computador cliente cuja lista de erros da criptografia de arquivos você deseja visualizar.

3. No espaço de trabalho, selecione a guia **Dispositivos**.

4. Na guia **Dispositivos** , selecione o nome do computador na lista e clique com o botão direito do mouse para abrir o menu de contexto.

5. Execute uma das seguintes ações:

   - No menu de contexto do computador, selecione **Proteção**.
   - No menu de contexto do computador, selecione o item **Propriedades**. Na janela **Propriedades: <nome do computador>**, selecione a seção **Proteção**.

6. Na seção **Proteção** da janela **Propriedades: <nome do computador>**, clique no link **Visualizar lista de erros de criptografia de dados** para abrir a janela **Erros de criptografia de dados**.

   Esta janela exibe detalhes dos erros de criptografia dos arquivos nas unidades do computador local. Quando um erro é corrigido, o Kaspersky Security Center remove os detalhes dos erros da janela **Erros de criptografia de dados**.

Exibir o relatório de criptografia de dados

Para visualizar o relatório de criptografia de dados:

1. Abra o Console de Administração do Kaspersky Security Center.
2. No nó **Servidor de administração** da árvore do Console de administração, selecione a guia **Relatórios**.
3. Clique no botão **Criar modelo de relatórios**.

   O Assistente de modelo de relatório é iniciado.

4. Siga as instruções do Assistente de Modelo de Relatório. Na janela **Selecionar tipo do modelo do relatório** na seção **Outra**, selecione um dos seguintes itens:

   - **Relatório de status de criptografia de dispositivo gerenciado**.
   - **Relatório de criptografia de dados de dispositivo armazenado**.
   - **Relatório de erros de criptografia**.
   - **Relatório de acesso bloqueado a arquivos criptografados**.

   Depois que você terminou com o Novo Assistente de Modelo de Relatório, o novo modelo de relatório aparece na tabela na guia **Relatórios**.

5. Selecione o modelo de relatório que foi criado nas etapas anteriores das instruções.

O processo de geração do relatório é iniciado. O relatório é exibido em uma nova janela.

Gerenciar arquivos criptografados com funcionalidade limitada de criptografia de arquivos

Quando a política do Kaspersky Security Center é aplicada e os arquivos são então criptografados, o Kaspersky Endpoint Security recebe uma chave de criptografia necessária para acessar os arquivos criptografados diretamente. Usando essa chave de criptografia, um usuário com qualquer conta Windows que esteve ativa durante a criptografia do arquivo pode acessar os arquivos criptografados diretamente. Um usuário com contas Windows que esteve inativo durante a criptografia do arquivo tem que se conectar ao Kaspersky Security Center para acessar os arquivos criptografados.

Os arquivos criptografados podem ser não acessíveis nas seguintes circunstâncias:

- O computador do usuário armazena chaves de criptografia, mas não há conexão ao Kaspersky Security Center para o gerenciamento das chaves. Neste caso, o usuário deve solicitar acesso aos arquivos criptografados junto ao administrador da rede local.

  Se o acesso ao Kaspersky Security Center não existir, você deve:

  - solicitar uma chave de acesso o acesso a arquivos criptografados em discos rígidos de computador;
  - para acessar arquivos criptografados que estão armazenados em unidades removíveis, solicite chaves de acesso em separado para arquivos criptografados em cada unidade removível.

- Os componentes de criptografia são excluídos do computador do usuário. Neste evento, o usuário pode abrir arquivos criptografados em discos removíveis e locais, mas os conteúdos daqueles arquivos parecerão criptografados.

  O usuário pode trabalhar com arquivos criptografados nas seguintes circunstâncias:

  - Os arquivos são colocados dentro de pacotes criptografados criados em um computador com o Kaspersky Endpoint Security instalado.
  - Os arquivos são armazenados em unidades removíveis nas quais o modo portátil foi permitido.

Acessar arquivos criptografados sem conexão ao Kaspersky Security Center

Estas instruções são destinadas para usuários de computadores de cliente com Kaspersky Endpoint Security instalado.

Para acessar arquivos criptografados sem conexão ao Kaspersky Security Center:

1. Tente acessar o arquivo criptografado que você precisa.

   Se não houver conexão com o Kaspersky Security Center quando você tentar acessar um arquivo armazenado em uma unidade local do computador, o Kaspersky Endpoint Security gera um arquivo com uma solicitação de acesso a todos os arquivos criptografados armazenados nas unidades do computador local. Se você tentar acessar um arquivo armazenado em uma unidade removível, o Kaspersky Endpoint Security gera um arquivo que solicita acesso a todos os arquivos criptografados armazenados na unidade removível. A janela **Acesso ao arquivo bloqueado** abre.

2. Envie o arquivo que contém, a solicitação de acesso a arquivos criptografados para o administrador de rede da área local. Para isso, execute uma das seguintes operações:

   - Para enviar o arquivo de solicitação de acesso a arquivos criptografados por e-mail para o administrador de rede local, clique no botão **Enviar por e-mail**
   - Para salvar o arquivo que solicita acesso aos arquivos criptografados e entregá-lo ao administrador da rede local por um método diferente, clique no botão **Salvar**.

3. Obtenha o arquivo de chave para acessar os arquivos criptografados, que foi criado e fornecido pelo administrador da rede local.

4. Ative a chave de acesso a arquivos criptografados de uma das seguintes maneiras:

- Em qualquer gerenciador de arquivos, selecione o arquivo da chave de acesso a arquivos criptografados. Abra-o com clique duplo.

- Faça o seguinte:

  a. Abra a janela principal do Kaspersky Endpoint Security.

  b. Clique no botão .

     Isso abre a janela **Eventos**.

  c. Selecione a guia **Status de acesso a arquivos e dispositivos**.

     A guia contém uma lista de todas as solicitações de acesso a arquivos criptografados.

  d. Selecione a solicitação para a qual você recebeu o arquivo de chave para acessar os arquivos criptografados.

  e. Para carregar o arquivo de chave fornecido para acessar arquivos criptografados, clique em **Procurar**.

     A caixa de diálogo padrão **Selecionar o arquivo da chave de acesso** do Microsoft Windows abre.

  f. Na janela **Selecionar o arquivo da chave de acesso** padrão do Microsoft Windows, selecione o arquivo fornecido pelos administradores com a extensão .kesdr e nome que combina com o nome de arquivo no arquivo de solicitação de acesso.

  g. Clique no botão **Abrir**.

  h. Na janela **Eventos**, clique em **OK**.

Se um arquivo com uma solicitação de acesso a arquivos criptografados é gerado durante uma tentativa de acesso a um arquivo armazenado em uma unidade local do computador, o Kaspersky Endpoint Security gera um arquivo com uma solicitação de acesso a todos os arquivos criptografados armazenados nas unidades do computador local. Se um arquivo de solicitação de acesso a arquivos criptografados é gerado durante uma tentativa de acesso a um arquivo armazenado em uma unidade removível, o Kaspersky Endpoint Security concede acesso a todos os arquivos criptografados armazenados na unidade removível. Para acessar arquivos criptografados armazenados em outras unidades removíveis, você deve obter um arquivo de chave de acesso em separado para cada unidade removível.

Conceder acessar a arquivos criptografados sem conexão ao Kaspersky Security Center

Para conceder acesso a arquivos criptografados sem uma conexão ao Kaspersky Security Center:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** da árvore de Console de Administração, abra a pasta com o nome do grupo de administração que inclui o computador do usuário que está solicitando acesso a arquivos criptografados.

3. No espaço de trabalho, selecione a guia **Dispositivos**.

4. Na guia **Dispositivos**, selecione o computador que pertence ao usuário que solicitou acesso aos arquivos criptografados e clique com o botão direito para abrir o menu de contexto.

5. No menu de contexto, selecione a opção **Conceder acesso a dispositivos e dados em modo off-line**.

   A janela **Conceder acesso a dispositivos e dados em modo off-line** é exibida.

6. Na janela **Conceder acesso a dispositivos e dados em modo off-line**, selecione a guia **Criptografia**.

7. Na guia **Criptografia**, clique no botão **Procurar**.

   A caixa de diálogo padrão **Selecionar o arquivo de solicitação de acesso** do Microsoft Windows é aberta.

8. Na janela **Selecionar o arquivo de solicitação de acesso**, especifique o caminho para o arquivo de solicitação recebido do usuário e clique em **Abrir**.

   O Kaspersky Security Center gera um arquivo de chave para acesso aos arquivos criptografados. Os detalhes da solicitação do usuário são exibidos na guia **Criptografia**.

9. Execute uma das seguintes ações:

   - Para enviar por e-mail o arquivo de chave gerado para o usuário, clique no botão **Enviar por e-mail**.
   - Para salvar o arquivo de chave de acesso a arquivos criptografados e entregá-lo ao usuário por um método diferente, clique no botão **Salvar**.

Editar modelos de mensagens de acesso a arquivos criptografados

Para editar modelos de mensagens de acesso a arquivos criptografados:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja editar os modelos de mensagens de solicitação de acesso a arquivos criptografados.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Selecione a política desejada.

5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

6. Na seção **Criptografia de dados**, selecione a subseção **Configurações comuns de criptografia**.

7. Na seção **Modelos**, clique no botão **Modelos**.

   A janela **Modelos** é exibida.

8. Faça o seguinte:

   - Se desejar editar o modelo de mensagem do usuário, selecione a guia **Mensagem do usuário**. A janela **Acesso ao arquivo negado** é exibida quando o usuário tentar acessar um arquivo criptografado enquanto não houver uma chave disponível no computador para acessar os arquivos criptografados. Clicar no botão **Enviar por e-mail** na janela **Acesso ao arquivo negado** cria automaticamente uma mensagem do usuário. Esta mensagem é enviada ao administrador de LAN corporativo junto com o arquivo solicitando acesso a arquivos criptografados.

- Se desejar editar o modelo de mensagem do administrador, selecione a guia **Mensagem do administrador**. Esta mensagem é criada automaticamente ao clicar no botão **Enviar por e-mail**, na janela **Conceder acesso a arquivos criptografados**, e é enviada ao usuário depois que o usuário receber acesso a esses arquivos.

9. Edite os modelos de mensagem.

   Você pode usar o botão **Padrão** e a lista suspensa **Variável**.

10. Clique em **OK**.

11. Para salvar as alterações, na janela **Propriedades: <Nome de política>**, clique em **OK**.

Trabalhar com dispositivos criptografados quando não há acesso a eles

Obter acesso a dispositivos bloqueados

Um usuário pode ter de solicitar o acesso a dispositivos criptografados nos seguintes casos:

- O disco rígido foi criptografado em um computador diferente.
- A chave de criptografia de um dispositivo não está no computador (por exemplo, depois da primeira tentativa de acessar a unidade removível criptografada no computador), e o computador não é conectado ao Kaspersky Security Center.

  Depois que o usuário tiver aplicado a chave de acesso ao dispositivo criptografado, o Kaspersky Endpoint Security salva a chave de criptografia no computador do usuário e permite o acesso a este dispositivo depois de tentativas de acesso subsequentes, mesmo se não houver conexão ao Kaspersky Security Center.

O acesso a dispositivos criptografados pode ser obtido assim:

1. O usuário usa a interface do aplicativo Kaspersky Endpoint Security para criar um arquivo de solicitação de acesso com a extensão kesdc e envia-o ao administrador da rede local corporativa.
2. O administrador usa o Console de Administração do Kaspersky Security Center para criar um arquivo de chave de acesso com a extensão kesdr e envia-o ao usuário.
3. O usuário aplica a chave de acesso.

Restaurar dados em dispositivos criptografados

Um usuário pode usar o Utilitário de Restauração de Dispositivo Criptografado (denominado aqui como Utilitário de Restauração) para trabalhar com dispositivos criptografados. Isso pode ser necessário nos seguintes casos:

- O procedimento para usar uma chave de acesso para obter acesso foi mal sucedido.
- Os componentes de criptografia não foram instalados no computador com o dispositivo criptografado.

Os dados necessários para restaurar o acesso a dispositivos criptografados usando o Utilitário de Restauração residem na memória do computador do usuário na forma não criptografada por algum tempo. Para reduzir o risco de acesso não autorizado a esses dados, é recomendável que você restaure o acesso a dispositivos criptografados em computadores confiáveis.

Os dados em dispositivos criptografados podem ser restaurados como se segue:

1. O usuário usa o Utilitário de Restauração para criar um arquivo de solicitação de acesso com a extensão fdertc e envia-o ao administrador da rede local corporativa.
2. O administrador usa o Console de Administração do Kaspersky Security Center para criar um arquivo de chave de acesso com a extensão fdertr e envia-o ao usuário.
3. O usuário aplica a chave de acesso.

Para restaurar dados em discos rígidos do sistema criptografado, o usuário também pode especificar as credenciais de conta do Agente de Autenticação no Utilitário de Restauração. Se os metadados da conta do Agente de Autenticação tiverem sido corrompidos, o usuário deve concluir o procedimento de restauração usando um arquivo de solicitação de acesso.

Antes de restaurar dados em dispositivos criptografados, recomenda-se cancelar a política de criptografia do Kaspersky Security Center do computador onde esta operação deve ser executada. Isso evita que a unidade seja criptografada novamente.

Obter acesso a dispositivos criptografados pela interface de aplicativo

Estas instruções são destinadas para usuários de computadores de cliente com Kaspersky Endpoint Security instalado.

Para obter acesso a dispositivos criptografados pela interface do aplicativo:

1. Tente acessar o dispositivo criptografado que você precisa.

   A janela **O acesso aos dados está bloqueado** se abre.

2. Envie ao administrador de rede local corporativo o arquivo de solicitação de acesso com a extensão kesdc para o dispositivo criptografado. Para isso, execute uma das seguintes operações:

   - Para enviar um e-mail ao administrador de rede local corporativa com o arquivo de solicitação de acesso gerado para o dispositivo criptografado, clique no botão **Enviar por e-mail**.
   - Para salvar o arquivo de solicitação de acesso para os arquivos criptografados e entregá-lo ao administrador da rede local por um método diferente, clique no botão **Salvar**.

   Se você tiver fechado a janela **O acesso aos dados está bloqueado** sem salvar o arquivo de solicitação de acesso ou sem enviá-lo ao administrador de rede local corporativa, você pode fazer isso a qualquer momento na janela **Eventos** da guia **Status de acesso a arquivos e dispositivos**. Para abrir esta janela, clique no botão na janela principal do aplicativo.

3. Obtenha e salve o arquivo chave de acesso ao dispositivo criptografado que foi criado e fornecido pelo administrador da rede local corporativa.
4. Use um dos seguintes métodos para aplicar a chave de acesso para acessar o dispositivo criptografado:

- Em qualquer gerenciador de arquivos, encontre o arquivo da chave de acesso a dispositivo criptografado e clique duas vezes nele para abri-lo.

- Faça o seguinte:

  a. Abra a janela principal do Kaspersky Endpoint Security.

  b. Clique no botão para abrir a janela **Eventos**.

  c. Selecione a guia **Status de acesso a arquivos e dispositivos**.

  A guia exibe uma lista de todas as solicitações de acesso a arquivos e dispositivos criptografados.

  d. Selecione a solicitação para a qual você recebeu o arquivo de chave de acesso para acessar o dispositivo criptografado.

  e. Para carregar o arquivo de chave de acesso fornecido para acessar o dispositivo criptografado, clique em **Procurar**.

  A caixa de diálogo padrão **Selecionar o arquivo da chave de acesso** do Microsoft Windows abre.

  f. Na janela **Selecionar o arquivo da chave de acesso** padrão do Microsoft Windows, selecione o arquivo fornecido pelo administrador com a extensão kesdr e o nome que combina com o nome de arquivo que corresponde ao arquivo de solicitação de acesso ao dispositivo criptografado.

  g. Clique no botão **Abrir**.

  h. Na janela **Status de acesso a arquivos e dispositivos**, clique em **OK**.

Como resultado, o Kaspersky Endpoint Security concede acesso ao dispositivo criptografado.

Conceder acesso de usuário a dispositivos criptografados

Para conceder acesso de usuário a um dispositivo criptografado:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração que inclui o computador do usuário que está solicitando acesso ao dispositivo criptografado.

3. No espaço de trabalho, selecione a guia **Dispositivos**.

4. Na guia **Dispositivos**, selecione o computador que pertence ao usuário que solicitou acesso ao dispositivo criptografado e clique com o botão direito para abrir o menu de contexto.

5. No menu de contexto, selecione a opção **Conceder acesso a dispositivos e dados em modo off-line**.

   A janela **Conceder acesso a dispositivos e dados em modo off-line** é exibida.

6. Na janela **Conceder acesso a dispositivos e dados em modo off-line**, selecione a guia **Criptografia**.

7. Na guia **Criptografia**, clique no botão **Procurar**.

   A caixa de diálogo padrão **Selecionar o arquivo de solicitação de acesso** do Microsoft Windows é aberta.

8. Na janela **Selecionar o arquivo de solicitação de acesso**, especifique o caminho para o arquivo de solicitação com a extensão kesdc que você recebeu do usuário.

9. Clique no botão **Abrir**.

   O Kaspersky Security Center gera um arquivo chave de acesso a dispositivo criptografado com a extensão kesdr. Os detalhes da solicitação do usuário são exibidos na guia **Criptografia**.

10. Execute uma das seguintes ações:

    - Para enviar por e-mail o arquivo de chave gerado para o usuário, clique no botão **Enviar por e-mail**.
    - Para salvar o arquivo de chave de acesso do dispositivo criptografado e entregá-lo ao usuário por outro método, clique no botão **Salvar**.

Fornecer a um usuário uma chave de recuperação de discos rígidos criptografados com BitLocker

Para enviar a um usuário uma chave de recuperação para um disco rígido de sistema que foi criptografado usando BitLocker:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, na pasta **Dispositivos gerenciados**, abra a pasta com o nome do grupo de administração que inclui o computador do usuário que está solicitando acesso à unidade criptografada.
3. No espaço de trabalho, selecione a guia **Dispositivos**.
4. Na guia **Dispositivos**, selecione o nome do computador que pertence ao usuário que está solicitando acesso à unidade criptografada.
5. Clique com o botão direito no menu de contexto, selecione **Conceder acesso a dispositivos e dados em modo off-line**.

   A janela **Conceder acesso a dispositivos e dados em modo off-line** é exibida.

6. Na janela **Conceder acesso a dispositivos e dados em modo off-line**, selecione a guia **Acesso a uma unidade do sistema protegida por BitLocker**.
7. Solicite ao usuário o ID de chave de recuperação indicado na janela de entrada de senha de BitLocker e compare-o com o ID no campo **ID da chave de recuperação**.

   Se os IDs não combinarem, essa chave não será válida para restaurar o acesso à unidade de sistema especificada. Assegure que o nome do computador selecionado combina com o nome do computador do usuário.

8. Envie ao usuário a chave que é indicada no campo **Chave de recuperação**.

Para enviar a um usuário uma chave de recuperação para um disco rígido de não-sistema que foi criptografado usando BitLocker:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore de Console de administração, selecione a pasta **Adicional** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.

   O espaço de trabalho exibe uma lista de dispositivos criptografados.

3. Na área de trabalho, selecione o dispositivo criptografado ao qual você precisa restituir o acesso.
4. Clique com o botão direito do mouse para exibir o menu de contexto e selecione **Conceder chave de acesso ao dispositivo criptografado especificado**.

   Isto abre a janela **Restaurar acesso a uma unidade criptografada com BitLocker**.
5. Solicite ao usuário o ID de chave de recuperação indicado na janela de entrada de senha de BitLocker e compare-o com o ID no campo **ID da chave de recuperação**.

   Se os IDs não combinarem, esta chave não será válida para restaurar o acesso à unidade especificada. Assegure que o nome do computador selecionado combina com o nome do computador do usuário.
6. Envie ao usuário a chave que é indicada no campo **Chave de recuperação**.

Criar o arquivo executável do Utilitário de Restauração

Estas instruções são destinadas para usuários de computadores de cliente com Kaspersky Endpoint Security instalado.

Para criar o arquivo executável do Utilitário de Restauração:

1. Abra a janela principal do aplicativo.
2. Clique no botão no canto inferior esquerdo da janela principal do aplicativo para abrir a janela **Suporte**.
3. Na janela **Suporte**, clique no botão **Restaurar dispositivo criptografado**.

   O Utilitário de Restauração de dispositivo criptografado é iniciado.
4. Clique no botão **Utiliário de criação de restauração independente** na janela do Utilitário de Restauração.

   A janela **Criando utilitário de Restauração independente** é exibida.
5. Na janela **Salvar em**, digite manualmente o caminho para a pasta para salvar o arquivo executável do Utilitário de Restauração, ou clique no botão **Procurar**.
6. Clique em **OK** na janela **Criando utilitário de Restauração independente**.

   O arquivo executável do Utilitário de Restauração (fdert.exe) é salvo na pasta selecionada.

Restaurando o acesso a dispositivos criptografados utilizando o Utilitário de Restauração

Estas instruções são destinadas para usuários de computadores de cliente com Kaspersky Endpoint Security instalado.

Para restaurar o acesso a um dispositivo criptografado usando o Utilitário de Restauração.

1. Execute a restauração de utilitário das seguintes formas:

   - Clicar no botão na janela principal do Kaspersky Endpoint Security para abrir a janela **Suporte** e clicar no botão **Restaurar dispositivo criptografado**.

   - Execute o arquivo executável fdert.exe do Utilitário de Restauração. Este arquivo é criado pelo Kaspersky Endpoint Security.

2. Na janela Utilitário de Restauração, na lista suspensa **Selecionar dispositivo**, selecione um dispositivo criptografado ao qual você deseja restaurar o acesso.

3. Clique no botão **Verificar** para permitir que o utilitário defina quais ações devem ser executadas no dispositivo: se ele deve ser desbloqueado ou descriptografado.

   Se o computador tiver acesso à funcionalidade de criptografia do Kaspersky Endpoint Security, o Utilitário de Restauração o avisa para desbloquear o dispositivo. Enquanto o desbloqueio do dispositivo não o descriptografar, o dispositivo se torna diretamente acessível como resultado do desbloqueio. Se o computador não tiver acesso à funcionalidade de criptografia do Kaspersky Endpoint Security, o Utilitário de Restauração o avisa para descriptografar o dispositivo.

4. Clique no botão **Corrigir MBR** caso o diagnóstico do disco rígido do sistema criptografado exiba uma mensagem de problemas envolvendo o registro de reinício mestre (MBR) do dispositivo.

   A correção do registro de reinício mestre do dispositivo pode acelerar o processo de recolha das informações necessárias para desbloquear ou descriptografar o dispositivo.

5. Clique no botão **Desbloquear** ou **Descriptografar** dependendo dos resultados do diagnóstico.

   A janela **Configurações de desbloqueio do dispositivo** ou **Configurações de descriptografia de dispositivos** é aberta.

6. Se você quiser restaurar dados usando uma conta de Agente de Autenticação:

   a. Selecione a opção de **Usar parâmetros de conta do Agente de Autenticação**.

   b. Nos campos **Nome** e **Senha**, especifique as credenciais de conta do Agente de Autenticação.

   Este método só é possível com a restauração dos dados em um disco rígido do sistema. Se o disco rígido do sistema foi corrompido e os dados de conta do Agente de Autenticação foram perdidos, você deve obter uma chave de acesso do administrador da rede local corporativa para restaurar os dados em um dispositivo criptografado.

7. Se você quer usar uma chave de acesso para restaurar dados:

   a. Selecione a opção **Especificar chave de acesso do dispositivo manualmente** opção.

   b. Clique no botão **Obter chave de acesso**.

   c. A janela **Receber chave de acesso do dispositivo** é aberta.

   d. Clique no botão **Salvar** e selecione a pasta na qual salvar o arquivo de solicitação de acesso com a extensão fdertc.

   e. Envie o arquivo de solicitação de acesso ao dispositivo ao administrador da rede local corporativa.

   Só feche a janela **Receber chave de acesso do dispositivo** após receber a chave de acesso. Quando esta janela for aberta novamente, você não conseguirá aplicar a chave de acesso que foi criada anteriormente pelo administrador.

f. Obtenha e salve o arquivo da chave de acesso que foi criada e fornecida pelo administrador da rede local corporativa.

g. Clique no botão **Carregar** e selecione o arquivo da chave de acesso com a extensão fdertr na janela que se abre.

8. Se estiver descriptografando um dispositivo, você também deve especificar outras configurações de descriptografia na janela **Configurações de descriptografia de dispositivos**. Para fazer isso:

   - Especifique a área a ser descriptografada:
     - Se você quiser descriptografar o dispositivo inteiro, selecione a opção **Descriptografar dispositivo inteiro**.
     - Se você quiser descriptografar uma parte dos dados em um dispositivo, selecione a opção **Descriptografar áreas individuais do dispositivo** e use os campos **Iniciar** e **Terminar** para especificar os limites da área de descriptografia.
   - Selecione a localização para gravar os dados descriptografados:
     - Se você quiser que os dados do dispositivo original sejam regravados com os dados descriptografados, desmarque a caixa de seleção **Salvar dados no arquivo após a descriptografia**.
     - Se você quiser salvar os dados descriptografados separadamente dos dados criptografados originais, marque a caixa de seleção **Salvar dados no arquivo após a descriptografia** e use o botão **Procurar** para especificar o caminho no qual salvar os dados.

9. Clique em **OK**.

O processo de desbloqueio/descriptografia do dispositivo é iniciado.

Respondendo a uma solicitação de usuário para restaurar dados em dispositivos criptografados

Para criar um arquivo de chave para acessar um dispositivo criptografado e fornecê-lo ao usuário:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore de Console de administração, selecione a pasta **Adicional** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.
3. Na área de trabalho, selecione o dispositivo criptografado para o qual você quer criar um arquivo chave de acesso e, no menu de contexto do dispositivo, selecione **Conceder chave de acesso ao dispositivo criptografado especificado**.

   Se você não tiver certeza de qual é o computador em que o arquivo de solicitação de acesso foi gerado, na árvore do Console de Administração, selecione a pasta **Adicional** → **Criptografia e proteção de dados** e, na área de trabalho, clique no link **Obter chave de criptografia**.

   A janela **Permitir acesso ao dispositivo** abre.

4. Selecione o algoritmo de criptografia em uso. Para isso, selecione uma das seguintes opções:

- **AES256**, se o Kaspersky Endpoint Security tiver sido instalado a partir de um pacote de distribuição localizado na pasta aes256 no computador em que o dispositivo foi criptografado;
- **AES56**, se o Kaspersky Endpoint Security tiver sido instalado a partir de um pacote de distribuição localizado na pasta aes56 no computador em que o dispositivo foi criptografado;

5. Clique no botão **Procurar**.

   A caixa de diálogo padrão **Selecionar o arquivo de solicitação de acesso** do Microsoft Windows é aberta.

6. Na janela **Selecionar o arquivo de solicitação de acesso**, especifique o caminho para o arquivo de solicitação com a extensão fdertc que você recebeu do usuário.

7. Clique no botão **Abrir**.

   O Kaspersky Security Center gera um arquivo chave de acesso com a extensão fdertr para acessar o dispositivo criptografado.

8. Execute uma das seguintes ações:
   - Para enviar por e-mail o arquivo de chave gerado para o usuário, clique no botão **Enviar por e-mail**.
   - Para salvar o arquivo de chave de acesso do dispositivo criptografado e entregá-lo ao usuário por outro método, clique no botão **Salvar**.

Restaurar o acesso a dados criptografados após falha no sistema operacional

Você pode restaurar o acesso aos dados após falha do sistema operacional somente para Criptografia a Nível de Arquivo (FLE, File Level Encryption). Você não pode restaurar o acesso aos dados se a Criptografia Completa do Disco (FDE, Full Disk Encryption) for usada.

Para restaurar o acesso a dados criptografados após falha no sistema operacional:

1. Reinstale o sistema operacional sem formatar o disco rígido.
2. Instalar o Kaspersky Endpoint Security.
3. Estabeleça uma conexão entre o computador e o Servidor de administração do Kaspersky Security Center que controlou o computador quando os dados foram criptografados.

O acesso aos dados criptografados será concedido sob as mesmas condições aplicadas antes da falha no sistema operacional.

Criar um disco de recuperação do sistema operacional

O disco de recuperação do sistema operacional pode ser útil quando um disco rígido criptografado não puder ser acessado por alguma razão e o sistema operacional não puser ser carregado.

Você pode carregar uma imagem do sistema operacional do Windows usando o disco de recuperação e restaurar o acesso ao disco rígido criptografado usando o Utilitário de Restauração incluído na imagem de sistema operacional.

Para criar um disco de recuperação do sistema operacional:

1. Crie um arquivo executável do Utilitário de Restauração de Dispositivo Criptografado.

2. Crie uma imagem personalizada do ambiente de pré-inicialização do Windows. Durante a criação da imagem personalizada do ambiente de pré-inicialização do Windows, adicione o arquivo executável do Utilitário de Restauração à imagem.

3. Salve a imagem personalizada do ambiente de pré-instalação do Windows em uma mídia executável, como um CD ou uma unidade removível.

   Consulte os arquivos de ajuda da Microsoft para obter instruções sobre a criação de uma imagem personalizada do ambiente pré-inicialização do Windows (por exemplo, no recurso do Microsoft TechNet).

Proteção da rede

Esta seção contém informações sobre o monitoramento do tráfego de rede e instruções sobre como definir as configurações das portas de rede monitoradas.

Sobre a Proteção da rede

Durante a operação do Kaspersky Endpoint Security, os componentes como Antivírus de E-mail, Antivírus da Web e Antivírus de MI monitoram os fluxos de dados que são transmitidos via protocolos específicos e que passam por portas TCP e UDP abertas no computador. Por exemplo, o Antivírus de E-mail verifica os dados que são transmitidos por SMTP, enquanto o Antivírus da Web verifica os dados que são transmitidos por protocolos HTTP e FTP.

O Kaspersky Endpoint Security divide as portas TCP e UDP do sistema operacional em vários grupos, de acordo com a probabilidade de comprometimento. Algumas portas de rede são reservadas para serviços que podem ser vulneráveis. É recomendável monitorar essas portas de forma exaustiva, pois é maior a probabilidade de ataque a elas. Se você usar serviços não padrão que dependem de portas de rede não padrão, estas portas de rede também poderão ser alvo de um computador atacante. É possível especificar uma lista de portas de rede e uma lista de aplicativos que exigem acesso de rede. Dessa forma, estas portas e estes aplicativos recebem atenção especial dos componentes de Antivírus de E-mail, Antivírus da Web e Antivírus de MI à medida que monitoram o tráfego de rede.

Definir as configurações do monitoramento do tráfego de rede

Você pode executar as seguintes ações para definir as configurações do monitoramento do tráfego de rede:

- Ativar o monitoramento de todas as portas de rede.
- Criar uma lista de portas de rede monitoradas.
- Criar uma lista de aplicativos para todas as portas de rede que são monitoradas.

Ativar o monitoramento de todas as portas de rede

Para ativar o monitoramento de todas as portas de rede:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção antivírus**.
   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na seção **Portas monitoradas**, selecione **Monitorar todas as portas de rede**.
4. Para salvar as alterações, clique no botão **Salvar**.

Criar uma lista de portas de rede monitoradas

Para criar uma lista de portas de rede monitoradas:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção antivírus**.

   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na seção **Portas monitoradas**, selecione **Monitorar somente portas selecionadas**.
4. Clique no botão **Configurações**.

   A janela **Portas de rede** é aberta. A janela **Portas de rede** exibe uma lista de portas de rede que são geralmente usadas para a transmissão de e-mail e tráfego de rede. Esta lista de portas de rede está incluída no pacote do Kaspersky Endpoint Security.
5. Nesta lista de portas de rede, execute as seguintes ações:

   - Marque as caixas de seleção ao lado das portas de rede que deseja incluir na lista de portas de rede monitoradas.

     Por padrão, são selecionadas as caixas de seleção ao lado de todas as portas de rede que estão listadas na janela **Portas de rede**.
   - Desmarque as caixas de seleção ao lado das portas de rede que deseja excluir da lista de portas de rede monitoradas.
6. Se a porta de rede não for exibida na lista de portas de rede, adicione-a da seguinte forma:

   a. Na lista de portas de rede, clique no link **Adicionar** para abrir a janela **Porta de rede**.

   b. Digite o número da porta de rede no campo **Porta**.

   c. Insira o nome da porta de rede no campo **Descrição**.

   d. Clique em **OK**.

      A janela **Porta de rede** é fechada. A nova porta de rede adicionada é exibida no final da lista de portas de rede.
7. Na janela **Portas de rede**, clique em **OK**.
8. Para salvar as alterações, clique no botão **Salvar**.

Quando o protocolo FTP é executado em modo passivo, a conexão pode ser estabelecida através de uma porta de rede aleatória que não é adicionada à lista de portas monitoradas. Para proteger tais conexões, selecione **Monitorar todas as portas de rede** na seção **Portas monitoradas** ou configura o monitoramento de todas as portas de aplicativos que estabelecem a conexão de FTP.

Criar uma lista de aplicativos para todas as portas de rede que são monitoradas

Você pode criar uma lista de aplicativos para os quais todas as portas de rede são monitoradas pelo Kaspersky Endpoint Security.

É recomendável incluir aplicativos que recebem ou transmitem dados via FTP na lista de aplicativos para os quais todas as portas de rede são monitoradas.

Para criar uma lista de aplicativos para os quais todas as portas de rede são monitoradas:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção antivírus**.

   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na seção **Portas monitoradas**, selecione **Monitorar somente portas selecionadas**.
4. Clique no botão **Configurações**.

   A janela **Portas de rede** é aberta.
5. Marque a caixa de seleção **Monitorar todas as portas dos aplicativos selecionados**.
6. Na lista de aplicativos na caixa de seleção **Monitorar todas as portas dos aplicativos selecionados**, faça o seguinte:

   - Marque as caixas de seleção ao lado dos nomes dos aplicativos para os quais você pretende monitorar todas as portas de rede.

     Por padrão, são marcadas as caixas de seleção ao lado de todos os aplicativos que estão listados na janela **Portas de rede**.

   - Desmarque as caixas de seleção ao lado dos nomes dos aplicativos para os quais você não pretende monitorar todas as portas de rede.
7. Se um aplicativo não estiver incluído na lista, adicione-o desta forma:

   a. Clique no link **Adicionar** na lista de aplicativos e abra o menu de contexto.

   b. No menu de contexto, selecione o modo para adicionar o aplicativo à lista:

      - Para selecionar um aplicativo na lista dos aplicativos que estão instalados no computador, selecione o comando **Aplicativos**. A janela **Selecionar aplicativo** é exibida, permitindo que você especifique o nome do aplicativo.

      - Para especificar a localização do arquivo executável do aplicativo, selecione o comando **Procurar**. A janela padrão **Abrir** no Microsoft Windows é exibida, permitindo que você especifique o nome do arquivo executável do aplicativo.

     A janela **Aplicativo** é aberta depois que você selecionar o aplicativo.

   c. No campo **Nome**, insira um nome para o aplicativo selecionado.

d. Clique em **OK**.

A janela **Aplicativo** é fechada. O aplicativo que você adicionou aparece no final da lista de aplicativos.

8. Na janela **Portas de rede**, clique em **OK**.

9. Para salvar as alterações, clique no botão **Salvar**.

Atualizar bancos de dados e módulos do software aplicativo

Esta seção contém informações sobre as atualizações dos bancos de dados e do módulo do aplicativo (também chamadas "atualizações") e as instruções para definir as configurações de atualização.

Sobre as atualizações do banco de dados e do módulo do aplicativo

A atualização dos bancos de dados e dos módulos do aplicativo do Kaspersky Endpoint Security assegura ao computador a versão de proteção mais recente. No mundo todo, novos tipos de vírus e malware surgem diariamente. Os bancos de dados do Kaspersky Endpoint Security contêm informações sobre ameaças e formas de neutralizá-las. Para detectar ameaças rapidamente, é necessário atualizar regularmente os bancos de dados e os módulos do aplicativo.

Atualizações frequentes exigem uma licença em vigor. Se não houver uma licença atual, será possível executar a atualização apenas uma vez.

Os servidores de atualização da Kaspersky são a principal fonte de atualização do Kaspersky Endpoint Security.

O computador precisa estar conectado à Internet para que o pacote de atualização possa ser baixado dos servidores de atualização da Kaspersky. Por padrão, as configurações de conexão com a Internet são definidas automaticamente. Se você usar um servidor proxy, é necessário ajustar as configurações de conexão.

Ao executar a atualização, os seguintes objetos são baixados e instalados no computador:

- Bancos de dados do Kaspersky Endpoint Security. A proteção do computador é fornecida utilizando bancos de dados com assinatura de vírus e outras ameaças e informações sobre a forma de neutralizá-las. Os componentes de proteção usam estas informações quando procuram e neutralizam arquivos infectados no computador. Os bancos de dados são constantemente atualizados com registros de novas ameaças e métodos para neutralizá-las. Portanto, é recomendável fazer a atualização dos bancos de dados regularmente.

  Além dos bancos de dados do Kaspersky Endpoint Security, também são atualizadas as unidades de rede que ativam os componentes do aplicativo de interceptação de tráfego de rede.

- Módulos do aplicativo. Além dos bancos de dados do Kaspersky Endpoint Security, faça também a atualização dos módulos do programa. A atualização dos módulos do aplicativo soluciona os problemas relativos a vulnerabilidades neste; adiciona novas funções ou aprimora as existentes.

Durante a atualização, os bancos de dados e os módulos do aplicativo no computador são comparados com a versão mais recente na fonte de atualização. Se forem encontradas diferenças nos bancos de dados e nos módulos do aplicativo, em relação às respectivas versões mais recentes, são instaladas as atualizações que faltam no computador.

Os arquivos de ajuda podem ser atualizados junto com os módulos do aplicativo.

Se os bancos de dados estão obsoletos, o pacote de atualização será grande, o que poderá causar tráfego de Internet (uma grande quantidade de Megabytes).

As informações sobre o status atual dos bancos de dados do Kaspersky Endpoint Security são exibidas em **Atualização** na seção **Tarefas** na guia **Proteção e controle** da janela principal do aplicativo.

As informações sobre resultados da atualização e sobre todos os eventos que ocorrem durante o desempenho da tarefa de atualização são registradas no relatório do Kaspersky Endpoint Security.

Sobre as fontes de atualização

A *fonte de atualização* é um recurso que contém as atualizações dos bancos de dados e dos módulos do aplicativo do Kaspersky Internet Security.

As fontes de atualização incluem o servidor do Kaspersky Security Center, servidores de atualização da Kaspersky e pastas de rede ou locais.

Configurações de atualização

Você pode executar as seguintes ações para configurar as definições de atualização:

- Adicionar novas fontes de atualização.

  A lista padrão de fontes de atualização inclui os servidores de atualização do Kaspersky Security Center e da Kaspersky. Você pode adicionar outras fontes de atualização à lista. Você pode especificar servidores FTP ou HTTP e pastas compartilhadas como fontes de atualização.

  Se vários recursos forem selecionados como fontes de atualização, o Kaspersky Endpoint Security tentará se conectar a cada um deles, começando pelo primeiro na lista, e executará a tarefa de atualização fazendo a recuperação do pacote de atualização da primeira fonte disponível.

  > Se um recurso externo à rede local for selecionado como fonte de atualização, será necessário ter uma conexão com a Internet para a atualização.

- Selecione a região do servidor de atualização da Kaspersky.

  Se os servidores de atualização da Kaspersky forem utilizados como fonte de atualização, selecione o local dos servidores de atualização da Kaspersky usados para fazer o download do pacote de atualização. Os servidores de atualização da Kaspersky estão localizados em diversos países. Usar os servidores de atualização da Kaspersky mais próximos ajuda a reduzir o tempo de recuperação do pacote de atualização.

  Por padrão, o aplicativo usa informações sobre a região atual do registro do sistema operacional.

- Configure a atualização do Kaspersky Endpoint Security a partir de uma pasta compartilhada.

  Para evitar tráfego de Internet, configure as atualizações do Kaspersky Endpoint Security para que os computadores na LAN recebam atualizações da pasta compartilhada. Para isso, um dos computadores na LAN recebe o pacote de atualização com as atualizações dos servidores de atualização do Kaspersky Security Center ou da Kaspersky e, em seguida, copia o pacote de atualização recuperado para uma pasta compartilhada. A partir de então, outros computadores na rede local poderão receber o pacote de atualização desta pasta compartilhada.

- Selecione o modo de execução da tarefa de atualização.

  Se não for possível executar a tarefa de atualização por qualquer motivo (por exemplo, o computador não está ligado no momento), você poderá configurar a tarefa ignorada para ser iniciada automaticamente assim que for possível.

  Você poderá adiar a execução da tarefa de atualização após o aplicativo iniciar se selecionar o modo de execução da tarefa de atualização **Por agendamento**, e se a hora de início do Kaspersky Endpoint Security corresponder à de início da tarefa de atualização programada. A tarefa de atualização somente pode ser executada após decorrido o intervalo de tempo especificado depois do início do Kaspersky Endpoint Security.

- Configure a tarefa de atualização para ser executada usando os direitos de uma conta de usuário diferente.

Adicionar uma fonte de atualização

Para adicionar uma fonte de atualização:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Atualização**.
   Na parte direita da janela, são exibidas as Configurações de Atualização do Aplicativo.
3. Na seção **Modo de execução e fonte de atualização**, clique no botão **Fonte de atualização**.
   A guia **Fonte** da janela **Atualização** é exibida.
4. Na guia **Fonte**, clique no botão **Adicionar**.
   A janela **Selecionar fonte de atualização** é exibida.
5. Na janela **Selecionar fonte de atualização**, selecione a pasta com o pacote de atualização ou insira o caminho completo para a pasta no campo **Fonte**.
6. Clique em **OK**.
7. Na janela **Atualização**, clique em **OK**.
8. Para salvar as alterações, clique no botão **Salvar**.

Selecionar a região do servidor de atualização

Para selecionar a região do servidor de atualização:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Atualização**.
   Na parte direita da janela, são exibidas as Configurações de Atualização do Aplicativo.
3. Na seção **Modo de execução e fonte de atualização**, clique no botão **Fonte de atualização**.
   A guia **Fonte** da janela **Atualização** é exibida.
4. Na guia **Fonte**, na seção **Configurações regionais**, selecione **Selecionar da lista**.
5. Na lista suspensa, selecione o país mais próximo do seu local atual.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Configurar atualizações de uma pasta compartilhada

A configuração das atualizações do Kaspersky Endpoint Security usando uma pasta compartilhada é constituída das seguintes etapas:

1. Ativação da ação de cópia do pacote de atualização para uma pasta compartilhada em um dos computadores na rede local.

2. Configuração de atualizações do Kaspersky Endpoint Security que são feitas em uma pasta compartilhada específica para os demais computadores na rede local.

Para ativar a cópia do pacote de atualização para a pasta compartilhada:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Atualização**.

   Na parte direita da janela, são exibidas as Configurações de Atualização do Aplicativo.

3. Na seção **Adicional**, marque a caixa de seleção **Copiar atualizações para pasta**.

4. Especifique o caminho para a pasta compartilhada em que o pacote de atualização será colocado. Isso pode ser feito das seguintes formas:

   - Digite o caminho para a pasta compartilhada no campo abaixo da caixa de seleção **Copiar atualizações para pasta**.

   - Clique no botão **Procurar**. Em seguida, na janela **Selecionar pasta** exibida, selecione a pasta desejada e clique em **OK**.

5. Para salvar as alterações, clique no botão **Salvar**.

Para configurar a atualização do Kaspersky Endpoint Security usando uma pasta compartilhada:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Atualização**.

   Na parte direita da janela, são exibidas as Configurações de Atualização do Aplicativo.

3. Na seção **Modo de execução e fonte de atualização**, clique no botão **Fonte de atualização**.

   A guia **Fonte** da janela **Atualização** é exibida.

4. Na guia **Fonte**, clique no botão **Adicionar**.

   A janela **Selecionar fonte de atualização** é exibida.

5. Na janela **Selecionar fonte de atualização**, selecione a pasta compartilhada que contém o pacote de atualização ou insira o caminho completo para a pasta compartilhada no campo **Fonte**.

6. Clique em **OK**.

7. Na guia **Fonte**, desmarque as caixas de seleção próximas aos nomes das fontes de atualização especificadas como pasta compartilhada.

8. Clique em **OK**.

9. Para salvar as alterações, clique no botão **Salvar**.

Selecionar o modo de execução da tarefa de atualização

Para selecionar o modo de execução da tarefa de atualização:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Atualização**.

   Na parte direita da janela, são exibidas as Configurações de Atualização do Aplicativo.

3. Clique no botão **Modo de execução**.

   A guia **Modo de execução** é exibida na janela **Atualização**.

4. Na seção **Modo de execução**, selecione uma das seguintes opções de execução da tarefa de atualização:

   - Para o Kaspersky Endpoint Security executar a tarefa de atualização de acordo com a disponibilidade do pacote de atualização na fonte de atualização, selecione **Automaticamente**. A frequência das verificações de pacotes de atualização pelo Kaspersky Endpoint Security aumenta quando há surtos de vírus e diminui quando estes não existem.

   - Se desejar executar a tarefa de atualização manualmente, selecione **Manualmente**.

   - Se desejar configurar a verificação programada para a tarefa de atualização, selecione **Por agendamento**.

5. Execute uma das seguintes ações:

   - Se tiver selecionado a opção **Automaticamente** ou **Manualmente**, vá para a etapa 6 destas instruções.

   - Se tiver selecionado a opção **Por agendamento**, especifique as configurações de execução da tarefa de atualização programada. Para fazer isso:

     a. Na lista suspensa **Frequência**, especifique a frequência da execução da tarefa de atualização. Selecione uma das seguintes opções: **Minutos**, **Horas**, **Dias**, **A cada semana**, **Em uma hora especificada**, **Todos os meses** ou **Após iniciar o aplicativo**.

     b. Especifique o valor que deseja usar nas configurações para definir a hora de início da tarefa de atualização, de acordo com o item selecionado na lista suspensa **Frequência**.

     c. No campo **Adiar a execução Após iniciar o aplicativo por**, especifique o intervalo de tempo de espera para iniciar a tarefa de atualização após a inicialização do Kaspersky Endpoint Security.

     > Se o item **Após iniciar o aplicativo** for selecionado na lista suspensa **Frequência**, o campo **Adiar a execução Após iniciar o aplicativo por** não estará disponível.

     d. Se desejar que o Kaspersky Endpoint Security execute as tarefas de atualização ignoradas assim que possível, marque a caixa de seleção **Executar tarefas ignoradas**.

Se **Horas**, **Minutos**, **Após iniciar o aplicativo** estiver selecionado na lista suspensa **Frequência**, a caixa de seleção **Executar tarefas ignoradas** não estará disponível.

6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Executar a tarefa de atualização usando os direitos de uma conta de usuário diferente

Por padrão, a tarefa de atualização do Kaspersky Endpoint Security é executada em nome da conta de usuário usada para fazer login no sistema operacional. Contudo, o Kaspersky Endpoint Security pode ser atualizado de uma fonte de atualização que o usuário não pode acessar por não ter os direitos de acesso (por exemplo, feitas em uma pasta compartilhada por meio de um pacote de atualização) ou por não ter os direitos de acesso de um servidor proxy autorizado. Nas configurações do Kaspersky Endpoint Security, especifique o usuário com os direitos necessários e execute a tarefa de atualização do aplicativo usando esta conta de usuário.

Para executar a tarefa de atualização com uma conta de usuário diferente:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Atualização**.
   Na parte direita da janela, são exibidas as Configurações de Atualização do Aplicativo.
3. Na seção **Modo de execução e fonte de atualização**, clique no botão **Modo de execução**.
   A guia **Modo de execução** é exibida na janela **Atualização**.
4. Na guia **Modo de execução**, na seção **Usuário**, selecione a caixa de seleção **Executar tarefa como**.
5. No campo **Nome**, insira o nome da conta do usuário que tem os direitos necessários para acessar a fonte de atualização.
6. No campo **Senha**, insira a senha do usuário que tem os direitos necessários para acessar a fonte de atualização.
7. Clique em **OK**.
8. Para salvar as alterações, clique no botão **Salvar**.

Configurar as atualizações dos módulos do aplicativo

Para configurar as atualizações do módulo do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Atualização**.
   Na parte direita da janela, são exibidas as Configurações de Atualização do Aplicativo.

3. Na seção **Adicional**, execute uma das seguintes operações:

   - Marque a caixa **Baixar atualizações dos módulos do aplicativo** se você desejar que o aplicativo inclua atualizações do módulo do aplicativo nos pacotes de atualização.

   - Caso contrário, desmarque a caixa seleção **Baixar atualizações dos módulos do aplicativo**.

4. Se a caixa de seleção **Baixar atualizações dos módulos do aplicativo** tiver sido selecionada na etapa anterior, especifique as condições nas quais o aplicativo instalará as atualizações de módulo do aplicativo:

   - Selecione a opção **Instalar atualizações críticas e confirmadas** se você desejar que o aplicativo instale atualizações críticas dos módulos do aplicativo automaticamente e quaisquer outras atualizações, se a sua instalação for aprovada, localmente, através da interface do aplicativo ou usando o Kaspersky Security Center.

   - Selecione a opção **Instalar somente atualizações confirmadas** se você desejar que o aplicativo instale atualizações dos módulos do aplicativo após sua instalação ser aprovada, localmente, através da interface do aplicativo ou usando o Kaspersky Security Center.

5. Para salvar as alterações, clique no botão **Salvar**.

Iniciar e interromper a tarefa de atualização

Seja qual for o modo de execução da tarefa de atualização, você pode iniciar ou interromper a tarefa de atualização do Kaspersky Endpoint Security a qualquer momento.

> É necessário ter uma conexão com a Internet para baixar um pacote de atualização dos servidores da Kaspersky.

Para iniciar ou interromper a tarefa de atualização:

1. Abra a janela principal do aplicativo.

2. Selecione a guia **Proteção e Controle**.

3. Clique na seção **Tarefas**.

   A seção **Tarefas** é exibida .

4. Clique com o botão direito do mouse para abrir a linha do menu de contexto com o nome da tarefa de atualização.

   Ao clicar nesta linha, é exibido um menu de ações da tarefa de atualização.

5. Execute uma das seguintes ações:

   - Se desejar iniciar a tarefa de atualização, selecione **Iniciar atualização** no menu.

     O status de andamento da tarefa de atualização, que é exibido à direita do botão **Atualização**, muda para *Em execução*.

   - Se desejar interromper a tarefa de atualização, selecione **Interromper atualização** no menu.

     O status de andamento da tarefa de atualização, que é exibido à direita do botão **Atualização**, muda para *Interrompido*.

Reverter a última atualização

Após a primeira atualização dos bancos de dados e dos módulos do aplicativo, é disponibilizada a função de reversão destes às respectivas versões anteriores.

A cada processo de atualização, o Kaspersky Endpoint Security cria uma cópia de backup dos bancos de dados e módulos do programa atuais. Dessa forma, é possível reverter os bancos de dados e os módulos do aplicativo às respectivas versões anteriores se for necessário. Reverter a última atualização é importante, por exemplo, quando a nova versão do banco de dados contém uma assinatura considerada inválida, ocasionando o bloqueio pelo Kaspersky Endpoint Security de um aplicativo seguro.

Para reverter a última atualização:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Tarefas**.
   A seção **Tarefas** é exibida .
4. Clique com o botão direito do mouse para abrir o menu de contexto da tarefa **Atualização**.
5. Selecione **Reverter atualização**.

Definir as configurações do servidor proxy

Para configurar o servidor proxy:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Atualização**.
   Na parte direita da janela, são exibidas as Configurações de Atualização do Aplicativo.
3. Na seção **Servidor proxy**, clique no botão **Configurações**.
   A janela **Configurações do servidor proxy** é exibida.
4. Na janela **Configurações do servidor proxy**, marque a caixa de seleção **Usar Servidor proxy**.
5. Defina as configurações do servidor proxy.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Você também pode definir as configurações do servidor proxy na janela principal do aplicativo, na guia **Configurações**, na seção **Configurações Avançadas**.

Verificar o computador

Uma verificação de vírus é uma parte essencial da segurança do computador. Executar verificações de vírus regularmente ajuda a eliminar a possibilidade de contaminação por malware que não é detectado pelos componentes de proteção devido à existência de um nível de segurança baixo ou por outros motivos.

Esta seção descreve as especificidades e configurações de tarefas de verificação, os níveis de segurança, os métodos e as tecnologias de verificação e as instruções para lidar com arquivos que o Kaspersky Endpoint Security não processou durante uma verificação de vírus.

Sobre as tarefas de verificação

Para encontrar vírus e outros tipos de malware e verificar a integridade dos módulos do aplicativo, o Kaspersky Endpoint Security inclui as seguintes tarefas:

- **Verificação Completa**. Uma verificação detalhada de todo o computador. Por padrão, o Kaspersky Endpoint Security verifica os seguintes objetos:
  - Memória Kernel
  - Os objetos que são carregados quando o sistema operacional é iniciado
  - Setores de inicialização
  - Backup do sistema operacional
  - Todos os discos rígidos e unidades removíveis
- **Verificação de Áreas Críticas**. Por padrão, o Kaspersky Endpoint Security verifica a memória kernel, os processos de execução e os setores de inicialização de disco.
- **Verificação Personalizada**. O Kaspersky Endpoint Security verifica os objetos que foram selecionados pelo usuário. Você pode verificar qualquer objeto da seguinte lista:
  - Memória Kernel
  - Os objetos que são carregados quando o sistema operacional é iniciado
  - Backup do sistema operacional
  - Caixa de e-mail do Outlook
  - Todos os discos rígidos, unidades removíveis e de rede
  - Qualquer arquivo selecionado
- **Verificação da integridade**. O Kaspersky Endpoint Security verifica os módulos do aplicativo para detectar corrupção ou modificações.

As tarefas de Verificação Completa e de Verificação de Áreas Críticas são um pouco diferentes das outras. Para essas tarefas, não é recomendado editar o escopo da verificação.

Após o início da tarefa de verificação, seu andamento será exibido no campo ao lado do nome da tarefa de verificação em execução, na seção **Tarefas** da guia **Proteção e Controle** da janela principal do Kaspersky Endpoint Security.

As informações sobre os resultados da verificação e os eventos que ocorreram durante a execução das tarefas de verificação serão exibidos num relatório do Kaspersky Endpoint Security.

Iniciar ou interromper uma tarefa de verificação

Independentemente do modo de execução da tarefa de verificação selecionado, é possível iniciar ou interromper uma tarefa de verificação em qualquer momento.

Para iniciar ou interromper uma tarefa de verificação:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Tarefas**.

   A seção **Tarefas** é exibida .
4. Clique com o botão direito do mouse para ser exibido o menu de contexto da linha com o nome da tarefa de verificação.

   É aberto um menu com as ações da tarefa de verificação.
5. Execute uma das seguintes ações:

   - Se pretender iniciar a tarefa de verificação, selecione **Iniciar verificação** no menu.

     O status do processo da tarefa que é exibido à direita do botão com o nome desta tarefa de execução muda para *Em execução*.

   - Se pretender interromper a tarefa de verificação, selecione **Interromper verificação** no menu.

     O status do processo da tarefa que é exibido à direita do botão com o nome desta tarefa de execução muda para *Interrompido*.

Definir as configurações da tarefa de verificação

Para definir as configurações da tarefa de verificação, faça o seguinte:

- Alterar o nível de segurança.

  Você pode selecionar um dos níveis de segurança pré-configurados ou definir manualmente configurações de nível de segurança. A alteração das configurações do nível de segurança não impede a reversão para as configurações de nível recomendado.

- Alterar a ação que o Kaspersky Endpoint Security executará se detectar um arquivo infectado.

- Editar o escopo da verificação.

  Você pode expandir ou restringir o escopo da verificação adicionando ou removendo objetos de verificação ou alterando o tipo dos arquivos a serem verificados.

- Otimizar a verificação.

  Pode otimizar a verificação dos arquivos: reduza o tempo da verificação e aumente a velocidade de processamento do Kaspersky Endpoint Security. Isso é possível quando são verificados apenas os arquivos novos e aqueles que foram alterados após a verificação anterior. Esse modo se aplica a arquivos simples e compostos. Você também pode limitar o tempo de verificação de um arquivo simples. Decorrido o intervalo de tempo especificado, o Kaspersky Endpoint Security exclui o arquivo da verificação atual (exceto arquivos compactados e objetos que incluem vários arquivos).

  Você também pode ativar o uso das tecnologias iChecker e iSwift. Estas tecnologias aumentam a velocidade das verificações por meio da exclusão de arquivos que permaneceram inalterados desde a última verificação.

- Configurar a verificação dos arquivos compostos.

- Configurar o uso dos métodos de verificação.

  Durante a verificação, o Kaspersky Endpoint Security usa a análise de assinaturas. Na análise de assinaturas, o Kaspersky Endpoint Security compara o objeto detectado com os registros do banco de dados. De acordo com as recomendações dos especialistas da Kaspersky, a análise de assinaturas está sempre ativada.

  Para aumentar a eficácia da proteção, você pode usar a análise heurística. Durante a análise heurística, o Kaspersky Endpoint Security analisa a atividade dos objetos no sistema operacional. A análise heurística consegue detectar objetos maliciosos ainda não registrados no banco de dados do Kaspersky Endpoint Security.

- Selecionar o modo de execução da tarefa de verificação.

  Se não for possível executar a tarefa de verificação por qualquer motivo (por exemplo, o computador não está ligado no momento), você poderá configurar a tarefa ignorada para iniciar automaticamente assim que for possível.

  Você poderá adiar a execução da tarefa de verificação após o aplicativo iniciar se tiver selecionado o modo de execução da tarefa de atualização **Por agendamento** e se a hora de execução do Kaspersky Endpoint Security corresponder à da tarefa de verificação programada. A tarefa de verificação somente pode ser executada após decorrido o intervalo de tempo especificado depois do início do Kaspersky Endpoint Security.

- Configurar a tarefa de verificação para ser executada usando os direitos de uma conta de usuário diferente.

- Especificar as configurações de verificação de unidades removíveis que estão conectadas.

Como alterar o nível de segurança

O Kaspersky Endpoint Security usa diversas combinações de configuração para executar tarefas de verificação. Essas combinações de configurações salvas no aplicativo são chamadas de *níveis de proteção*. Há três níveis de segurança pré-configurados: **Alto**, **Recomendado** e **Baixo**. As configurações de nível de segurança **Recomendado** são consideradas ótimas. Elas são recomendadas pelos peritos da Kaspersky.

Para modificar um nível de segurança:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione a subseção com o nome da tarefa de verificação desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, as configurações da tarefa de verificação desejada serão apresentadas.

3. Na seção **Nível de segurança**, execute uma das seguintes operações:

- Se você quiser aplicar um dos níveis de segurança pré-configurados (**Alto**, **Recomendado** ou **Baixo**), selecione-o com o controle deslizante.
- Se quiser configurar um nível de segurança de arquivos personalizado, clique no botão **Configurações** e especifique as configurações com o nome da tarefa de verificação.

  Após configurar um nível de segurança personalizado, o nome do nível de segurança, na seção de **Nível de segurança**, muda para **Personalizado**.
- Se quiser alterar o nível de segurança de e-mails para **Recomendado**, clique no botão **Padrão**.

4. Para salvar as alterações, clique no botão **Salvar**.

Alterar a ação a executar em arquivos infectados

Para alterar a ação a executar em arquivos infectados:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione a subseção com o nome da tarefa de verificação desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, as configurações da tarefa de verificação desejada serão apresentadas.
3. Na seção **Ação ao detectar ameaça**, selecione a opção desejada:
   - **Selecionar ação automaticamente**.
   - **Executar ação**.
4. Se tiver selecionado a opção **Executar ação** na etapa anterior, selecione as seguintes caixas:
   - Marque a caixa de seleção **Desinfectar** se você desejar que o Kaspersky Endpoint Security desinfecte os objetos nos quais foram detectadas ameaças.

     Ainda que esta opção não esteja selecionada, o Kaspersky Endpoint Security aplica a ação **Remover** aos arquivos que são parte do aplicativo Windows Store.
   - Marque a caixa de seleção **Excluir** se você desejar que o Kaspersky Endpoint Security exclua os objetos nos quais foram detectadas ameaças.
   - Marque as caixas de seleção **Desinfectar** e **Excluir** se você desejar que o Kaspersky Endpoint Security tente desinfetar os objetos nos quais as ameaças foram detectadas e excluir os objetos que não puderam ser desinfetados.
   - Desmarque as caixas de seleção **Desinfectar** e **Excluir** se você desejar que o Kaspersky Endpoint Security não tome nenhuma ação em objetos nos quais são detectadas ameaças, mas em vez disso, somente notifique o usuário sobre os resultados da verificação desses objetos.
5. Para salvar as alterações, clique no botão **Salvar**.

Gerar uma lista de objetos a verificar

Para gerar uma lista de objetos a verificar, você pode usar um destes seguintes métodos:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

> Este método está só disponível para tarefas **Verificação Completa** e **Verificação de Áreas Críticas**. A lista de objetos a verificar para a tarefa **Verificação Personalizada** só pode ser criada na guia **Proteção e Controle**.

Para ativar ou desativar a lista de objetos a verificar na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Tarefas**.

   A seção **Tarefas** é exibida .
4. Clique com o botão direito do mouse para abrir o menu de contexto da linha que contém o nome da tarefa e selecione **Escopo da verificação**.

   A janela **Escopo da verificação** é exibida.
5. Se desejar adicionar um novo objeto ao escopo da verificação:

   a. Clique no botão **Adicionar**.

      A janela **Selecionar escopo da verificação** é exibida.

   b. Selecione o objeto e clique em **Adicionar**.

      Todos os objetos que forem selecionados na janela **Selecionar escopo da verificação** são exibidos na lista **Escopo da verificação**.

   c. Clique em **OK**.
6. Se desejar alterar o caminho para um objeto no escopo da verificação:

   a. Selecione o objeto no escopo da verificação.

   b. Clique no botão **Editar**.

      A janela **Selecionar escopo da verificação** é exibida.

   c. Insira o novo caminho para o objeto no escopo da verificação.

   d. Clique em **OK**.
7. Se desejar remover um objeto do escopo da verificação:

   a. Selecione o objeto que deseja remover do escopo da verificação.

Para selecionar diversos objetos, selecione-os enquanto mantém pressionada a tecla **CTRL**.

b. Clique no botão **Remover**.

É exibida uma janela para confirmar exclusão.

c. Clique em **Sim** na janela de confirmação da remoção.

Você não pode remover ou editar objetos que estão incluídos no escopo da verificação padrão.

8. Para excluir um objeto do escopo da verificação, desmarque a caixa de seleção próxima ao objeto na janela **Escopo da verificação**.

O objeto permanece na lista de objetos no escopo da verificação, mas ele não é verificado quando a tarefa de verificação é executada.

9. Clique em **OK**.

10. Para salvar as alterações, clique no botão **Salvar**.

Para criar uma lista de objetos a verificar da janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione a subseção com o nome da tarefa desejada (**Verificação completa**, ou **Verificação de Áreas Críticas**).

Na parte direita da janela, as configurações da tarefa de verificação desejada serão apresentadas.

3. Clique no botão **Escopo da verificação**.

A janela **Escopo da verificação** é exibida.

4. Crie uma lista de objetos a verificar segundo as etapas 5-10 das instruções anteriores.

Selecionar o tipo de arquivos a verificar

Você pode usar estes dois métodos para selecionar o tipo de arquivos a verificar:

- Na guia **Proteção e Controle** da janela principal do aplicativo
- Na janela de configurações do aplicativo

Este método está só disponível para tarefas **Verificação Completa** e **Verificação de Áreas Críticas**. O tipo de arquivos a verificar para a tarefa **Verificação Personalizada** só pode ser selecionado na guia **Proteção e Controle**.

Para criar o tipo de arquivos a verificar na guia Proteção e Controle da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.

2. Selecione a guia **Proteção e Controle**.

3. Clique na seção **Tarefas**.

   A seção **Tarefas** é exibida .

4. Clique com o botão direito do mouse para abrir o menu de contexto da linha que contém o nome da tarefa e selecione **Configurações**.

   Abre uma janela com o nome da tarefa de verificação desejada.

5. Na janela com o nome da tarefa de verificação desejada, selecione a guia **Escopo**.

6. Na seção **Tipos de arquivos**, especifique o tipo dos arquivos que deseja verificar ao executar a tarefa de verificação:

   - Para verificar todos os arquivos, selecione **Todos os arquivos**.
   - Para verificar os arquivos nos formatos com risco maior de infecção, selecione **Arquivos verificados por formato**.
   - Se desejar verificar os arquivos com as extensões com risco maior de infecção, selecione **Arquivos verificados por extensão**.

   Ao selecionar o tipo dos arquivos a verificar, considere o seguinte:

   - Existem alguns formatos de arquivos (como .TXT) em que há uma baixa probabilidade de intrusão de código malicioso e ativação subsequente. Ao mesmo tempo, há formatos de arquivos que contêm ou que talvez contenham um código executável (como .exe, .dll e doc). O risco de infiltração e ativação de código malicioso nesses arquivos é grande.
   - O invasor talvez envie vírus ou outro tipo de programa malicioso para o computador em um arquivo executável renomeado com a extensão .txt. Se você selecionar a verificação de arquivos por extensão, o aplicativo ignora esse arquivo durante a verificação. Se a verificação de arquivos por formato for selecionada, o Antivírus de Arquivos analisa o cabeçalho do arquivo independentemente da extensão. Se esta análise revelar que o arquivo tem o formato de EXE, o aplicativo o verifica.

7. Na janela com o nome da tarefa de verificação, clique em **OK**.

8. Para salvar as alterações, clique no botão **Salvar**.

Para selecionar o tipo de arquivos a verificar na janela de configuração do aplicativo:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione a subseção com o nome da tarefa desejada (**Verificação completa**, ou **Verificação de Áreas Críticas**).

   Na parte direita da janela, as configurações da tarefa de verificação desejada serão apresentadas.

3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   Abre uma janela com o nome da tarefa de verificação desejada.

4. Na janela com o nome da tarefa de verificação desejada, selecione a guia **Escopo**.

5. Execute as etapas 5-7 das instruções anteriores.

Otimizar a verificação do arquivo

Para otimizar a verificação de arquivos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione a subseção com o nome da tarefa de verificação desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, as configurações da tarefa de verificação desejada serão apresentadas.
3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   Abre uma janela com o nome da tarefa de verificação desejada.
4. Na janela exibida, selecione a guia **Escopo**.
5. Na seção **Otimização da verificação**, executar as seguintes ações:
   - Marque a caixa de seleção **Verificar somente arquivos novos e alterados**.
   - Marque a caixa de seleção **Ignorar arquivos que são verificados por mais do que** e especifique a duração da verificação de um arquivo simples (em segundos).
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Verificar arquivos compostos

Um método comum para ocultar vírus e outro tipo de malware é incorporá-los em arquivos compostos, como arquivos compactados e bancos de dados. Para detectar vírus e outro tipo de malware que estão ocultos dessa forma, é necessário descompactar os arquivos compostos, o que pode reduzir a velocidade da verificação. É possível restringir os tipos dos arquivos compostos a verificar, o que aumentará a velocidade da verificação.

Para configurar a verificação de arquivos compostos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione a subseção com o nome da tarefa de verificação desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, as configurações da tarefa de verificação desejada serão apresentadas.
3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   Abre uma janela com o nome da tarefa de verificação desejada.
4. Na janela exibida, selecione a guia **Escopo**.
5. Na seção **Verificação de arquivos compostos**, especifique os arquivos compostos a verificar: arquivos, pacotes de instalação, arquivos em formatos do Office, arquivos de mensagem e arquivos compactados protegidos por senha.
6. Se a caixa de seleção **Verificar somente arquivos novos e alterados** estiver desmarcada na seção **Otimização da verificação**, clique no link **todos/novo** ao lado do nome do tipo de arquivo composto, se você quiser especificar para cada tipo do arquivo composto se devem ser verificados todos os arquivos desse tipo ou apenas os arquivos novos desse tipo.

Este link modifica o seu valor quando for clicado.

Se a caixa de seleção **Verificar somente arquivos novos e alterados** estiver selecionada, apenas os arquivos novos serão verificados.

7. Clique no botão **Adicional**.

   A janela **Arquivos compostos** é exibida.

8. Na seção **Limite de tamanho**, execute uma das seguintes operações:

   - Se não desejar descompactar os arquivos compostos grandes, marque a caixa de seleção **Não descompactar arquivos compostos grandes** e especifique o valor desejado no campo **Tamanho máximo de arquivo**.
   - Se desejar descompactar os arquivos compostos grandes, independentemente de seu tamanho, desmarque a caixa de seleção **Não descompactar arquivos compostos grandes**.

   O Kaspersky Endpoint Security verifica os arquivos grandes que foram extraídos dos arquivos compactados, independentemente de a caixa de seleção **Não descompactar arquivos compostos grandes** estar marcada.

9. Clique em **OK**.
10. Na janela com o nome da tarefa de verificação, clique em **OK**.
11. Para salvar as alterações, clique no botão **Salvar**.

Usar métodos de verificação

Para usar métodos de verificação:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione a subseção com o nome da tarefa de verificação desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, as configurações da tarefa de verificação desejada serão apresentadas.

3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   Abre uma janela com o nome da tarefa de verificação desejada.

4. Na janela exibida, selecione a guia **Adicional**.
5. Se desejar que o aplicativo use a análise heurística ao executar a tarefa de verificação, na seção **Métodos de verificação**, marque a caixa de seleção **Análise Heurística**. Em seguida, use o controle deslizante para definir o nível da análise heurística: **verificação superficial**, **verificação média** ou **verificação profunda**.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Usar tecnologias de verificação

Usar tecnologias de verificação:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione a subseção com o nome da tarefa de verificação desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, as configurações da tarefa de verificação desejada serão apresentadas.
3. Na seção **Nível de segurança**, clique no botão **Configurações**.

   Abre uma janela com o nome da tarefa de verificação desejada.
4. Na janela exibida, selecione a guia **Adicional**.
5. Na seção **Tecnologias de verificação**, marque as caixas de seleção junto aos nomes das tecnologias que deseja usar na verificação.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Selecionar o modo de execução da tarefa de verificação

Para selecionar o modo de execução da tarefa de verificação:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione a subseção com o nome da tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, as configurações da tarefa de verificação desejada serão apresentadas.
3. Clique no botão **Modo de execução**.

   Uma janela com as propriedades da tarefa selecionada é aberta na guia **Modo de execução**.
4. Na seção **Modo de execução**, selecione o modo de execução da tarefa: **Manualmente** ou **Por agendamento**.
5. Se você selecionou a opção **Por agendamento**, especifique as configurações do agendamento. Para fazer isso:

   a. Na lista suspensa **Frequência**, selecione a frequência de execução da tarefa (**Minutos**, **Horas**, **Dias**, **Todas as semanas**, **Em uma hora especificada**, **Todos os meses**, ou **Após iniciar o aplicativo**, **Após cada atualização**).

   b. Dependendo da frequência selecionada, defina configurações avançadas que especificam o agendamento da execução da tarefa.

   c. Se desejar que o Kaspersky Endpoint Security execute as tarefas de verificação ignoradas assim que possível, marque a caixa de seleção **Executar tarefas ignoradas**.

Se o item **Minutos**, **Horas**, **Após iniciar o aplicativo** ou **Após cada atualização** estiver marcado na lista suspensa **Frequência**, a caixa de seleção **Executar tarefas ignoradas** não estará disponível.

a. Se desejar que o Kaspersky Endpoint Security suspenda uma tarefa quando houver limitação de recursos do sistema, marque a caixa de seleção **Executar apenas quando o computador estiver ocioso**.

   Esta opção de agendamento ajuda a conservar recursos do computador.

6. Clique em **OK**.

7. Para salvar as alterações, clique no botão **Salvar**.

Iniciar uma tarefa de verificação com uma conta de um usuário diferente

Por padrão, a tarefa de verificação é executada com as permissões da conta na qual o usuário está registrado no sistema operacional. Contudo, talvez seja necessário executar a tarefa de verificação usando uma conta de usuário diferente. Especifique o usuário com os direitos necessários nas configurações da tarefa de verificação e execute a tarefa de verificação usando esta conta de usuário.

Para configurar a execução de uma tarefa de verificação usando uma conta de usuário diferente:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione a subseção com o nome da tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, as configurações da tarefa de verificação desejada serão apresentadas.

3. Clique no botão **Modo de execução**.

   Isso abre uma janela com as propriedades da tarefa selecionada na guia **Modo de execução**.

4. Na guia **Modo de execução**, na seção **Usuário**, selecione a caixa de seleção **Executar tarefa como**.

5. No campo **Nome**, insira o nome da conta do usuário cujos direitos são necessários para iniciar a tarefa de verificação.

6. No campo **Senha**, insira a senha do usuário que tem os direitos necessários para executar a tarefa de verificação.

7. Clique em **OK**.

8. Para salvar as alterações, clique no botão **Salvar**.

Verificar unidades removíveis quando conectadas ao computador

Alguns programas maliciosos exploram as vulnerabilidades do sistema operacional para serem replicados em redes locais e unidades removíveis. O Kaspersky Endpoint Security permite verificar unidades removíveis conectadas ao computador para detectar vírus e outro tipo de malware.

Para configurar a verificação de unidades removíveis conectadas ao computador:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Tarefas agendadas**.

   As configurações da tarefa são exibidas na parte direita da janela.
3. Na seção **Verificar unidades removíveis ao conectar**, na lista suspensa **Ação em conexão de unidades removíveis**, selecione a ação desejada:

   - **Não verificar**
   - **Verificação detalhada**

     Nesse modo, o Kaspersky Endpoint Security verifica todos os arquivos localizados na unidade removível, inclusive arquivos dentro de objetos compostos.
   - **Verificação rápida**

     Neste modo, o Kaspersky Endpoint Security verifica somente arquivos potencialmente infectáveis e não descompacta objetos compostos.
4. Se você desejar que o Kaspersky Endpoint Security verifique somente unidades removíveis cujo tamanho não exceda o valor especificado, marque a caixa de seleção **Tamanho máximo da unidade removível** e especifique um valor em megabytes no campo ao lado.
5. Para salvar as alterações, clique no botão **Salvar**.

Administrar arquivos não processados

Esta seção contém instruções sobre como administrar arquivos infectados e provavelmente infectados que não foram processados pelo Kaspersky Endpoint Security durante a verificação do computador para detectar vírus e outras ameaças.

Sobre os arquivos não processados

O Kaspersky Endpoint Security registra informações sobre arquivos que não foram processados por algum motivo. Estas informações são registradas em eventos na lista de arquivos não processados.

O arquivo infectado é considerado *processado* se o Kaspersky Endpoint Security executa uma das seguintes ações neste arquivo de acordo com as configurações do aplicativo durante a verificação do computador para detectar vírus e outras ameaças:

- Desinfectar.
- Remover.
- Excluir se a desinfecção falhar.

O arquivo infectado será considerado *não processado* se o Kaspersky Endpoint Security tiver falhado ao executar uma ação neste arquivo de acordo com as configurações especificadas do aplicativo durante a verificação do computador para detectar vírus e outras ameaças.

Esta situação ocorre nos seguintes casos:

- O arquivo verificado não está disponível (por exemplo, está localizado em uma unidade de rede ou em uma unidade removível sem privilégios de gravação).
- A ação que está selecionada na seção **Ação ao detectar ameaça** das tarefas de verificação é **Informar** e o usuário seleciona a ação **Ignorar** quando é exibida uma notificação sobre o arquivo infectado.

É possível iniciar manualmente uma tarefa de Verificação Personalizada na lista de arquivos não processados após atualizar os bancos de dados e os módulos do aplicativo. O status do arquivo poderá mudar após a verificação. Você tem a opção de executar as ações necessárias nos arquivos, dependendo do status destes.

Por exemplo, é possível executar as seguintes ações:

- Excluir arquivos com o status *Infectado*
- Restaure arquivos infectados que contêm informações importantes e restaure arquivos marcados como *Desinfectado* ou *Não infectado*.
- Arquivos de Quarentena com status *Provavelmente infectado*.

Gerenciar a lista de arquivos não processados

A lista de arquivos não processados aparece em uma tabela.

Você pode executar as seguintes operações com arquivos não processados:

- Exibir a lista de arquivos não processados.
- Verificar arquivos não processados usando a versão atual dos bancos de dados e módulos do Kaspersky Endpoint Security.
- Restaurar arquivos da lista de arquivos não processados para a pasta de origem ou para uma pasta diferente de sua escolha (quando não for possível gravar na pasta de origem).
- Remover arquivos da lista de arquivos não processados.
- Abrir a pasta de origem do arquivo não processado.

Também é possível efetuar as seguintes ações ao gerenciar dados na tabela:

- Filtrar os eventos de arquivos não processados por valores da coluna ou por condições de filtragem personalizadas.
- Utilizar a função de busca de evento de arquivo não processado.
- Classificar eventos de arquivos não processados.
- Alterar a ordem e a configuração das colunas que são exibidas na lista de eventos de arquivos não processados.
- Formar grupos de eventos de arquivos não processados.

É possível copiar os eventos de arquivos não processados desejados para área de transferência, se necessário.

Executar uma tarefa de Verificação Personalizada para arquivos não processados

Você pode iniciar manualmente a tarefa de Verificação Personalizada para arquivos não processados. Você pode iniciar a verificação se, por exemplo, a última verificação tiver sido interrompida por algum motivo ou se desejar voltar a verificar arquivos não processados após a última atualização de bancos de dados e módulos de aplicativos.

Para executar uma tarefa de Verificação Personalizada para arquivos não processados:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.
3. Na janela **Armazenamentos**, selecione a guia **Arquivos não processados**.
4. Na tabela da guia **Arquivos não processados**, selecione um ou mais eventos associados aos arquivos que deseja verificar.

   Para selecionar diversos eventos, selecione-os enquanto mantém pressionada a tecla **CTRL**.
5. Inicie a tarefa de Verificação Personalizada da seguinte forma:

   - Clique no botão **Verificar novamente**.
   - Clique com o botão direito do mouse para exibir o menu de contexto e selecione **Verificar novamente**.

Excluir arquivos da lista de arquivos não processados

Para excluir arquivos da lista de arquivos não processados:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.
3. Na janela **Armazenamentos**, selecione a guia **Arquivos não processados**.
4. Na tabela na guia **Arquivos não processados**, selecione um ou mais eventos envolvendo arquivos que você deseja excluir.

   Para selecionar diversos eventos, selecione-os enquanto mantém pressionada a tecla **CTRL**.
5. Exclua arquivos das seguintes formas:

   - Clique no botão **Remover**.
   - Clique com o botão direito para abrir o menu de contexto e selecione **Excluir**.

Verificação de Vulnerabilidades

Esta seção contém informações sobre as especificidades e configurações da tarefa de Verificação de Vulnerabilidades, bem como as instruções para o gerenciamento da lista de vulnerabilidades detectadas pelo Kaspersky Endpoint Security na execução da tarefa de Verificação de Vulnerabilidades.

Visualizar informações sobre as vulnerabilidades de aplicativos em execução

As informações sobre vulnerabilidades dos aplicativos em execução estarão disponíveis se o Kaspersky Endpoint Security for instalado em um computador que executa em Microsoft Windows para estações de trabalho. Estas informações estão disponíveis quando o Kaspersky Endpoint Security está instalado em um computador que executa em Microsoft Windows para servidores de arquivos

Para visualizar as informações sobre as vulnerabilidades de aplicativos em execução:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Abra a seção **Controle de Endpoints**.
4. Clique no botão **Monitoramento de atividades do aplicativo**.

   A janela **Controle de Privilégios de Aplicativo** é exibida na guia **Monitoramento de atividades do aplicativo**. A tabela **Monitoramento de atividades do aplicativo** mostra informações resumidas sobre a atividade dos aplicativos que estão em execução no sistema operacional. A gravidade da vulnerabilidade dos aplicativos em execução, conforme determinada pelo componente Monitoramento de Vulnerabilidades, é exibida na coluna **Gravidade da vulnerabilidade**.

Sobre a tarefa de Verificação de Vulnerabilidades

As vulnerabilidades do sistema operacional podem ser causadas, por exemplo, por erros de agendamento ou design, senhas de baixa segurança e atividades de malware. Ao verificar vulnerabilidades, o aplicativo analisa o sistema operacional e procura anomalias e configurações danificadas de aplicativos do Microsoft e de outros fornecedores.

A verificação de vulnerabilidades executa o diagnóstico de proteção do sistema operacional e detecta recursos de software que podem ser usados por invasores para disseminar objetos maliciosos e obter acesso a informações pessoais.

Após o início da tarefa de Verificação de Vulnerabilidades, seu andamento é exibido no campo ao lado do nome da tarefa de **Verificação de Vulnerabilidades** na seção **Tarefas**, na guia **Proteção e Controle** da janela principal do Kaspersky Endpoint Security.

Os resultados da tarefa de Verificação de Vulnerabilidades são registrados em relatórios.

Iniciar ou interromper a tarefa de Verificação de Vulnerabilidades

É possível iniciar ou interromper a tarefa de verificação de vulnerabilidades a qualquer momento, seja qual for o modo de execução.

Para iniciar ou interromper uma tarefa de verificação de vulnerabilidades:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Clique na seção **Tarefas**.

   A seção **Tarefas** é exibida .
4. Clique com o botão direito do mouse para exibir o menu de contexto da linha com o nome da tarefa de Verificação de Vulnerabilidades.

   É exibido um menu de operações da tarefa de Verificação de Vulnerabilidades.
5. Execute uma das seguintes ações:

   - Para executar a tarefa de Verificação de Vulnerabilidades, selecione **Iniciar verificação** no menu.

     O status de andamento da tarefa que é exibido à direita do botão com o nome da tarefa de Verificação de Vulnerabilidades muda para *Em execução*.

   - Para interromper a tarefa de Verificação de Vulnerabilidades, selecione **Interromper verificação** no menu.

     O status de andamento da tarefa que é exibido à direita do botão com o nome da tarefa de Verificação de Vulnerabilidades muda para *Interrompido*.

Definir as configurações de Verificação de Vulnerabilidades

Para definir as configurações de Verificação de Vulnerabilidades, faça o seguinte:

- Crie o escopo da Verificação de Vulnerabilidades.

  Você pode expandir ou estreitar o escopo da verificação adicionando ou removendo aplicativos para serem verificados quanto a vulnerabilidades.

- Selecione o modo de execução da tarefa de Verificação de Vulnerabilidades

  Se não for possível executar a tarefa de verificação por qualquer motivo (por exemplo, o computador não está ligado no momento), você poderá configurar a tarefa ignorada para executar automaticamente assim que for possível.

- Configure a tarefa para ser executada usando os direitos de uma conta de usuário diferente.

  Por padrão, a tarefa de verificação é executada com as permissões da conta na qual o usuário está registrado no sistema operacional. Contudo, talvez seja necessário executar a tarefa de verificação usando uma conta de usuário diferente. Você pode especificar o usuário com os direitos necessários nas configurações da tarefa e executar a tarefa usando essa conta de usuário.

Criar o escopo da verificação de vulnerabilidades

O escopo da verificação de vulnerabilidades é um fornecedor de software ou o caminho para a pasta onde o software foi instalado (por exemplo, todos os aplicativos Microsoft que foram instalados na pasta Arquivos de Programas).

Para criar um escopo da verificação de vulnerabilidades:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Verificação de vulnerabilidades**.

   Na parte direita da janela, são exibidas as configurações da tarefa de Verificação de vulnerabilidades.
3. Na seção **Escopo da verificação**:

   a. Para usar o Kaspersky Endpoint Security para buscar vulnerabilidades em aplicativos Microsoft que estão instalados no computador, selecione a caixa **Microsoft**.

   b. Para usar o Kaspersky Endpoint Security para buscar vulnerabilidades em todos os aplicativos Microsoft que estão instalados no computador para além dos da Microsoft, selecione a caixa **Outros fornecedores**.

   c. Na janela **Área de verificação de vulnerabilidade adicional**, clique no botão **Configurações**.

   A janela **Escopo da verificação de vulnerabilidades** é exibida.

   d. Crie o escopo da verificação de vulnerabilidades. Para fazer isso, utilize os botões **Adicionar** e **Remover**.

   e. Na janela **Escopo da verificação de vulnerabilidades**, clique em **OK**.
4. Para salvar as alterações, clique no botão **Salvar**.

Selecionar o modo de execução da tarefa de Verificação de Vulnerabilidades

Para selecionar o modo de execução da tarefa de verificação de vulnerabilidades:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Verificação de vulnerabilidades**.

   Na parte direita da janela, são exibidas as configurações da tarefa de Verificação de vulnerabilidades.
3. Clique no botão **Modo de execução**.

   Isso abre a guia **Modo de execução** da janela **Verificação de vulnerabilidades**.
4. Na seção **Modo de execução**, selecione uma das seguintes opções de modo de execução para a tarefa de Verificação de vulnerabilidades:

   - Se desejar executar a tarefa de Verificação de vulnerabilidades manualmente, selecione **Manualmente**.
   - Se desejar configurar a verificação programada para a tarefa de verificação de vulnerabilidades, selecione **Por agendamento**.
5. Execute uma das seguintes ações:

   - Se tiver selecionado a opção **Manualmente**, vá para a etapa 6 destas instruções.

- Se tiver selecionado a opção **Por agendamento**, especifique as configurações de execução da tarefa de Verificação de vulnerabilidades. Para fazer isso:

  a. Na lista suspensa **Frequência**, especifique quando executar a tarefa de Verificação de vulnerabilidades. Selecione uma das seguintes opções: **Dias**, **Todas as semanas**, **Em uma hora especificada**, **Todos os meses**, **Após iniciar o aplicativo** ou **Após cada atualização**.

  b. Especifique os valores que deseja usar nas configurações para definir a hora de início da tarefa de Verificação de Vulnerabilidades, de acordo com o item selecionado na lista suspensa **Frequência**.

  c. Se desejar que o Kaspersky Endpoint Security execute as tarefas de Verificação de Vulnerabilidades ignoradas assim que possível, marque a caixa de seleção **Executar tarefas ignoradas**

  > Se a opção **Após iniciar o aplicativo** ou **Após cada atualização** estiver selecionada na lista suspensa **Frequência**, a caixa de seleção **Executar tarefas ignoradas** não estará disponível.

6. Clique em **OK**.

7. Para salvar as alterações, clique no botão **Salvar**.

Iniciar a tarefa de Verificação de Vulnerabilidades usando os direitos de uma conta de usuário diferente

Por padrão, a tarefa de Verificação de Vulnerabilidades é executada com a conta na qual o usuário está registrado no sistema operacional. Contudo, talvez seja necessário executar a tarefa de Verificação de vulnerabilidades usando uma conta de usuário diferente. Especifique o usuário com os direitos necessários nas configurações da tarefa de Verificação de Vulnerabilidades e execute a tarefa usando essa conta de usuário.

Para configurar o início da tarefa de Verificação de vulnerabilidades com uma conta de usuário diferente:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Verificação de vulnerabilidades**.

   Na parte direita da janela, são exibidas as configurações da tarefa de Verificação de vulnerabilidades.

3. Clique no botão **Modo de execução**.

   Isso abre a guia **Modo de execução** da janela **Verificação de vulnerabilidades**.

4. Na guia **Modo de execução**, na seção **Usuário**, selecione a caixa de seleção **Executar tarefa como**.

5. No campo **Nome**, insira o nome da conta do usuário que tem os direitos necessários para executar a tarefa de Verificação de vulnerabilidades.

6. No campo **Senha**, insira a senha do usuário que tem os direitos necessários para executar a tarefa de Verificação de vulnerabilidades.

7. Clique em **OK**.

8. Para salvar as alterações, clique no botão **Salvar**.

Gerenciar a lista de vulnerabilidades

Ao gerenciar a lista de vulnerabilidades, é possível executar as seguintes ações:

- Exibir a lista de vulnerabilidades.
- Iniciar a tarefa de verificação de vulnerabilidades novamente após atualizar os bancos de dados e os módulos do aplicativo.
- Exibir informações detalhadas sobre a vulnerabilidade e as recomendações para corrigi-la em uma seção separada.
- Ocultar as entradas selecionadas na lista de vulnerabilidades.
- Filtrar a lista de vulnerabilidades por grau de importância.
- Filtrar a lista de vulnerabilidades por valores de status *Corrigido* e *Oculto*.

Também é possível efetuar as seguintes ações ao gerenciar dados na tabela:

- Filtrar a lista de vulnerabilidades por valores da coluna ou por condições de filtragem personalizadas.
- Usar a função de busca de vulnerabilidades.
- Classificar as entradas na lista de vulnerabilidades.
- Alterar a ordem e a configuração das colunas que são exibidas na lista de vulnerabilidades.
- Colocar as entradas em grupos na lista de vulnerabilidades.

Sobre a lista de vulnerabilidades

O Kaspersky Endpoint Security registra os resultados da tarefa de Verificação de vulnerabilidades na lista de vulnerabilidades.

Depois que você examinar as vulnerabilidades específicas e executar as ações que são recomendadas para corrigi-las, o Kaspersky Endpoint Security altera o status das vulnerabilidades para *Corrigido*.

Se você não deseja exibir as entradas sobre vulnerabilidades específicas na lista de vulnerabilidades, é possível ocultá-las. O Kaspersky Endpoint Security atribui o status *Oculto* a estas vulnerabilidades.

A lista de vulnerabilidades aparece em uma tabela. Cada linha da tabela contém as seguintes informações:

- Um ícone que significa o nível de gravidade da vulnerabilidade. Os níveis de gravidade das vulnerabilidades são os seguintes:
  - Ícone ⚠. **Crítico**. Este nível de gravidade aplica-se às vulnerabilidades com grau alto de risco que deverão ser corrigidas imediatamente. Os intrusos exploram ativamente as vulnerabilidades desse nível para infectar o sistema operacional do computador ou acessar os dados pessoais do usuário. A Kaspersky recomenda que você realize imediatamente todas as etapas necessárias para corrigir as vulnerabilidades do nível de gravidade “Crítico”.

- Ícone . **Importante**. Este nível de gravidade aplica-se às vulnerabilidades importantes que deverão ser corrigidas em breve. Os intrusos podem explorar ativamente as vulnerabilidades deste nível. Os intrusos atualmente não exploram ativamente as vulnerabilidades do nível de gravidade "Importante". A Kaspersky recomenda que você realize imediatamente todas as etapas necessárias para corrigir as vulnerabilidades do nível de gravidade "Importante".

- Ícone . **Aviso**. Este nível de gravidade aplica-se às vulnerabilidades que podem ser corrigidas posteriormente. No entanto, tais vulnerabilidades podem ameaçar a segurança do computador no futuro.

- ID da vulnerabilidade.
- Nome do aplicativo em que a vulnerabilidade foi detectada.
- Breve descrição da vulnerabilidade.
- Informações sobre o fabricante do software, conforme indicado na assinatura digital.
- Resultado de ações empreendidas para corrigir a vulnerabilidade.

Iniciar a tarefa de verificação de vulnerabilidades novamente

Para atualizar informações sobre vulnerabilidades detectadas anteriormente, você pode reiniciar a tarefa de Verificação de Vulnerabilidades. Pode ser necessário reiniciar a tarefa de verificação se a verificação de vulnerabilidades tiver sido interrompida por algum motivo ou se você desejar verificar o computador em busca de vulnerabilidades depois da última atualização dos bancos de dados e dos módulos do aplicativo.

Para iniciar a tarefa de Verificação de Vulnerabilidades novamente:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.
3. Na janela **Armazenamentos**, selecione a guia **Vulnerabilidades**.

   A guia **Vulnerabilidades** contém uma lista de vulnerabilidades que foram detectadas pelo Kaspersky Endpoint Security durante a tarefa de verificação de vulnerabilidades.
4. No canto inferior direito da janela **Armazenamentos**, clique no botão **Verificar novamente**.

   O Kaspersky Endpoint Security atualiza informações detalhadas sobre vulnerabilidades na lista de vulnerabilidades.

O status da vulnerabilidade que foi corrigida após a instalação de uma correção recomendada não altera após ser feita outra verificação de vulnerabilidades.

Corrigir uma vulnerabilidade

É possível corrigir uma vulnerabilidade instalando a atualização do sistema operacional, alterando a configuração do aplicativo ou instalando uma correção de aplicativo.

As vulnerabilidades detectadas talvez não sejam aplicadas a aplicativos instalados, mas a cópias destes. A correção pode corrigir uma vulnerabilidade somente se o aplicativo estiver instalado.

Para corrigir uma vulnerabilidade:

1. Abra a janela principal do aplicativo.

2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.

3. Na janela **Armazenamentos**, selecione a guia **Vulnerabilidades**.

   A guia **Vulnerabilidades** contém uma lista de vulnerabilidades que foram detectadas pelo Kaspersky Endpoint Security durante a tarefa de verificação de vulnerabilidades.

4. Na lista de vulnerabilidades, selecione a entrada que corresponde àquela desejada.

   Uma seção com informações sobre essa vulnerabilidade e recomendações sobre como consertá-la abre na parte de baixo da lista de vulnerabilidades.

   É possível encontrar as seguintes informações em todas as vulnerabilidade selecionadas:

   - Nome do aplicativo em que a vulnerabilidade foi detectada.
   - Versão do aplicativo em que a vulnerabilidade foi detectada.
   - Nível de gravidade de uma vulnerabilidade.
   - ID da vulnerabilidade.
   - Data e hora da última vulnerabilidade detectada.
   - Recomendações para corrigir a vulnerabilidade (por exemplo, o link para um site para encontrar a atualização do sistema operacional ou a correção de aplicativo).
   - Link para um site com a descrição da vulnerabilidade.

5. Para ver a descrição detalhada da vulnerabilidade, clique no link **Informações adicionais** para abrir a página contendo a descrição da ameaça que está associada à vulnerabilidade selecionada. O site www.secunia.com permite baixar e instalar a atualização necessária para a versão atual do aplicativo.

6. Selecione um dos seguintes meios para corrigir a vulnerabilidade:

   - Se mais de uma correção estiver disponível para o aplicativo, instale aquele que é necessário seguindo as instruções que estão do lado do nome da correção.
   - Se estiver disponível uma atualização do sistema operacional, instale a atualização necessária seguindo as instruções fornecidas ao lado do nome da atualização.

   A vulnerabilidade é corrigida após você instalar a correção ou a atualização. O Kaspersky Endpoint Security atribui a essa vulnerabilidade o status que indica que a vulnerabilidade está corrigida. A entrada referente à correção da vulnerabilidade é exibida em cinza na lista de vulnerabilidades.

7. Se não houver nenhuma informação sobre como corrigir uma vulnerabilidade na parte inferior da janela, será possível iniciar a tarefa de Verificação de Vulnerabilidades novamente após a atualização dos bancos de dados e dos módulos do Kaspersky Endpoint Security. Como o Kaspersky Endpoint Security verifica o sistema para

detectar vulnerabilidades com base no banco de dados de vulnerabilidades, talvez apareça uma entrada referente a uma vulnerabilidade corrigida após a atualização do aplicativo.

Ocultar entradas na lista de vulnerabilidades

É possível ocultar uma entrada de vulnerabilidade selecionada. O Kaspersky Endpoint Security atribui o status *Oculto* às entradas selecionadas na lista de vulnerabilidades e assinaladas como ocultas. Em seguida, você pode filtrar a lista da vulnerabilidade pelo valor de status *Oculto*.

Para ocultar uma entrada na lista de vulnerabilidades:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.
3. Na janela **Armazenamentos**, selecione a guia **Vulnerabilidades**.

   A guia **Vulnerabilidades** contém uma lista de vulnerabilidades que foram detectadas pelo Kaspersky Endpoint Security durante a tarefa de verificação de vulnerabilidades.
4. Na lista de vulnerabilidades, selecione a entrada sobre a vulnerabilidade que você deseja ocultar.

   Uma seção com informações sobre essa vulnerabilidade e recomendações sobre como consertá-la abre na parte de baixo da lista de vulnerabilidades.
5. Clique no botão **Ocultar**.

   O Kaspersky Endpoint Security atribui o status *Oculto* à vulnerabilidade selecionada. Entradas sobre vulnerabilidades com o status *Oculto* são movidas para o fim da lista de vulnerabilidades e destacadas a cinza.
6. Para ocultar uma entrada sobre uma vulnerabilidade na lista de vulnerabilidades, marque a caixa de seleção **Oculto** na parte superior da lista.

Filtrar a lista de vulnerabilidades por nível de gravidade

Para filtrar a lista de vulnerabilidades por nível de gravidade:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.
3. Na janela **Armazenamentos**, selecione a guia **Vulnerabilidades**.

   A guia **Vulnerabilidades** contém uma lista de vulnerabilidades que foram detectadas pelo Kaspersky Endpoint Security durante a tarefa de verificação de vulnerabilidades. Três ícones do nível de gravidade das vulnerabilidades (Aviso, Importante, Crítico) aparecem na parte superior da lista de vulnerabilidades na linha **Exibir gravidade**. Ao clicar nesses ícones, você poderá filtrar a lista de vulnerabilidades por nível de gravidade.
4. Clique em um, dois ou três ícones do nível de gravidade da vulnerabilidade. As vulnerabilidades correspondem aos níveis de gravidade selecionados que são exibidos na lista. Para deixar de mostrar as vulnerabilidades que correspondem a um nível de gravidade específico na lista, clique no ícone do nível de gravidade relevante novamente. Se nenhum nível de gravidade for selecionado, a lista de vulnerabilidades ficará vazia.

As condições do filtro da entrada de vulnerabilidades especificadas são salvas depois de você fechar a janela **Armazenamentos**.

Filtrar a lista de vulnerabilidades por valores de status Corrigido e Oculto

Para filtrar a lista de vulnerabilidades por valores de status Corrigido e Oculto:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.
3. Na janela **Armazenamentos**, selecione a guia **Vulnerabilidades**.

   A guia **Vulnerabilidades** contém uma lista de vulnerabilidades que foram detectadas pelo Kaspersky Endpoint Security durante a tarefa de verificação de vulnerabilidades.
4. As caixas de seleção que indicam o status das vulnerabilidades são exibidas ao lado da configuração **Exibir vulnerabilidades**. Para filtrar a lista de vulnerabilidades por status *Corrigido*, faça o seguinte:

   - Para exibir entradas de vulnerabilidades corrigidas na lista de vulnerabilidades, marque a caixa de seleção **Corrigido**. As entradas relativas a vulnerabilidades corrigidas são exibidas em cinza na lista de vulnerabilidades.
   - Para ocultar entradas de vulnerabilidades corrigidas na lista de vulnerabilidades, desmarque a caixa de seleção **Corrigido**.
5. Para filtrar a lista de vulnerabilidades por status *Oculto*, faça o seguinte:

   - Para exibir entradas de vulnerabilidades ocultas na lista de vulnerabilidades, marque a caixa de seleção **Oculto**. As entradas relativas a vulnerabilidades ocultas são exibidas em cinza na lista de vulnerabilidades.
   - Para ocultar entradas de vulnerabilidades ocultas na lista de vulnerabilidades, desmarque a caixa de seleção **Oculto**.

As condições de filtragem da entrada de vulnerabilidade especificada não são salvas depois de você fechar a janela **Armazenamentos**.

Verificar a integridade dos módulos do aplicativo

Esta seção contém informações sobre a especificação e as configurações da tarefa de verificação da integridade.

Sobre a tarefa de Verificação da Integridade

O Kaspersky Endpoint Security verifica os módulos do aplicativo na pasta de instalação do aplicativo para detectar corrupção ou modificações. Se um módulo do aplicativo tiver uma assinatura digital incorreta, o módulo é considerado corrompido.

Após o início da tarefa de verificação da integridade, seu andamento é exibido no campo ao lado do nome da tarefa na seção **Tarefas** na guia **Proteção e Controle** da janela principal do Kaspersky Endpoint Security.

Os resultados da tarefa de verificação da integridade são registrados em relatórios.

Iniciar ou interromper uma tarefa de verificação da integridade

Independentemente do modo de execução selecionado, é possível iniciar ou interromper uma tarefa de verificação em qualquer momento.

Para iniciar ou interromper uma tarefa de verificação da integridade:

1. Abra a janela principal do aplicativo.
2. Selecione a guia **Proteção e Controle**.
3. Abra a seção de **Tarefas**.
4. Clique com o botão direito do mouse para exibir o menu de contexto da linha com o nome da tarefa de verificação da integridade.
5. Execute uma das seguintes ações:
   - Para iniciar a tarefa de verificação da integridade, selecione **Iniciar verificação** no menu de contexto.

     O status do processo da tarefa que é exibido à direita do botão com o nome dessa tarefa muda para *Em execução*.
   - Se você pretender interromper a tarefa de verificação da integridade, selecione **Interromper verificação** no menu de contexto.

     O status do processo da tarefa que é exibido à direita do botão com o nome dessa tarefa muda para *Interrompido*.

Selecionar o modo de execução da tarefa de verificação da integridade

Para selecionar o modo de execução da tarefa de verificação da integridade:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Tarefas agendadas**, selecione **Verificação da integridade**.

   Na parte direita da janela, são exibidas as configurações da tarefa de Verificação da integridade.
3. Na seção **Modo de execução**, selecione uma das seguintes opções:

   - Se desejar iniciar a tarefa de verificação da integridade manualmente, selecione **Manualmente**.
   - Se desejar configurar o agendamento do início da tarefa de verificação da integridade, selecione **Por agendamento**.
4. Se você tiver selecionado a opção **Por agendamento** na etapa anterior, especifique as configurações do agendamento da execução da tarefa. Para fazer isso:

   a. Na lista suspensa **Frequência**, especifique quando a tarefa de verificação da integridade deve ser iniciada. Selecione uma das seguintes opções: **Minutos**, **Horas**, **Dias**, **A cada semana**, **Em uma hora especificada**, **Todos os meses** ou **Após iniciar o aplicativo**.

   b. Especifique o valor que deseja usar nas configurações para definir a hora de início da tarefa, de acordo com o item selecionado na lista suspensa **Frequência**.

   c. Se desejar que o Kaspersky Endpoint Security inicie as tarefas de verificação da integridade ignoradas assim que possível, marque a caixa de seleção **Executar tarefas ignoradas**.

   > Se o item **Horas**, **Minutos** ou **Após iniciar o aplicativo** estiver marcado na lista suspensa **Frequência**, a caixa de seleção **Executar tarefas ignoradas** não estará disponível.

   d. Se desejar que o Kaspersky Endpoint Security suspenda uma tarefa quando houver limitação de recursos do sistema, marque a caixa de seleção **Executar apenas quando o computador estiver ocioso**.

   Esta opção de agendamento ajuda a conservar recursos do computador.
5. Clique em **OK**.
6. Para salvar as alterações, clique no botão **Salvar**.

Gerenciar relatórios

Esta seção descreve como definir as configurações de relatórios e gerenciar os relatórios.

Generalidades do gerenciamento de relatórios

As informações sobre a operação de cada componente do Kaspersky Endpoint Security, o desempenho de cada tarefa de verificação, a tarefa de atualização, a tarefa de controle de integridade, a tarefa de verificação de vulnerabilidades e o funcionamento do aplicativo de forma geral são registrados em relatórios.

Os dados do relatório são apresentados em uma tabela que contém uma lista de eventos. Cada linha da tabela contém informações sobre um evento diferente. Os atributos do evento estão dispostos nas colunas da tabela. Algumas colunas são compostas, contendo colunas aninhadas que incluem atributos adicionais. Para exibir atributos adicionais, você deve pressionar o botão ⊞ ao lado do nome do gráfico. Os eventos registrados na execução dos diversos componentes ou o desempenho de várias tarefas têm conjuntos de atributos diferentes.

Os seguintes relatórios estão disponíveis:

- Relatório de **Auditoria do Sistema**. Contém informações sobre os eventos ocorridos durante a interação entre usuário e aplicativo e durante a execução do aplicativo em geral, que não estão relacionadas a nenhum componente ou tarefa do Kaspersky Endpoint Security em particular.
- Relatório de **todos os componentes de proteção**. Contém informações sobre os eventos que são registrados durante a execução dos seguintes componentes do Kaspersky Endpoint Security:
  - Antivírus de Arquivos
  - Antivírus de e-mail.
  - Antivírus da Web.
  - Antivírus de MI.
  - Inspetor do Sistema.
  - Firewall.
  - Bloqueio de Ataque de Rede.
  - Prevenção contra ataque BadUSB.
- Relatório sobre a execução de um componente do Kaspersky Endpoint Security ou a realização de uma tarefa.
- Relatório de **Criptografia**. Contém informações sobre eventos que ocorrem durante a criptografia e descriptografia de dados.

Os relatórios utilizam os seguintes níveis de importância de eventos:

- **Eventos informativos**. Ícone . Eventos para fins de informação que geralmente não são de importância crítica.
- **Eventos importantes**. Ícone . Eventos que exigem atenção porque representam situações importantes na execução do Kaspersky Endpoint Security.

- **Eventos críticos**. Ícone . Eventos de importância crítica que indicam problemas no funcionamento do Kaspersky Endpoint Security ou vulnerabilidades na proteção do computador do usuário.

Para trazer praticidade ao processamento de relatórios, é possível modificar a apresentação dos dados na tela da seguinte forma:

- Filtrar a lista de eventos usando vários critérios.
- Utilizar a função de busca para encontrar um determinado evento.
- Exibir o evento selecionado em uma seção separada.
- Ordenar a lista de eventos por cada coluna do relatório.
- Exibir e ocultar eventos agrupados pelo filtro de evento.
- Alterar a ordem e a configuração das colunas exibidas no relatório.

É possível salvar um relatório gerado em arquivo de texto, se necessário.

Você também pode excluir as informações do relatório sobre componentes e tarefas do Kaspersky Endpoint Security que estão arranjadas em grupos. O Kaspersky Endpoint Security exclui todas as entradas dos relatórios selecionados da entrada mais antiga até a data atual.

Definir as configurações de relatório

Você pode definir as configurações de relatório das seguintes formas:

- Configurar o período máximo de armazenamento de relatórios.

  O período máximo padrão de armazenamento de relatórios sobre eventos registrados pelo Kaspersky Endpoint Security é de 30 dias. Após este período, o Kaspersky Endpoint Security exclui as entradas mais antigas do arquivo de relatório automaticamente. Você pode cancelar a restrição de tempo ou alterar a duração máxima do armazenamento de relatórios.

- Configurar o tamanho máximo do arquivo de relatório.

  Você pode especificar o tamanho máximo do arquivo que contém o relatório. Por padrão, o tamanho máximo do arquivo de relatório é 1.024 MB. Para evitar ultrapassar o tamanho máximo do arquivo de relatório, o Kaspersky Endpoint Security exclui as entradas mais antigas do arquivo de relatório automaticamente quando for ultrapassado o tamanho máximo. Você pode cancelar a restrição ao tamanho do arquivo de relatório ou definir um valor diferente.

Configurar o período máximo de armazenamento de relatórios

Para modificar o período máximo de armazenamento de relatórios:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Configurações Avançadas**, selecione **Relatórios e armazenamentos**.
3. Na parte direita da janela, na seção **Parâmetros do relatório**, execute uma das seguintes ações:

- Para limitar o período máximo de armazenamento de relatórios, marque a caixa de seleção **Armazenar relatórios por no máximo**. No campo próximo à caixa de seleção **Armazenar relatórios por no máximo**, especifique o período máximo de armazenamento dos relatórios.

  O período máximo padrão de armazenamento dos relatórios é de 30 dias.

- Para cancelar a limitação do período máximo de armazenamento de relatórios, desmarque o botão **Armazenar relatórios por no máximo**.

A limitação do período máximo de armazenamento de relatórios está ativada, por padrão.

4. Para salvar as alterações, clique no botão **Salvar**.

Configurar o tamanho máximo do arquivo de relatório

Para configurar o tamanho máximo do arquivo de relatório:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Configurações Avançadas**, selecione **Relatórios e armazenamentos**.
3. Na parte direita da janela, na seção **Parâmetros do relatório**, execute uma das seguintes ações:

   - Para limitar o tamanho do arquivo de relatório, marque a caixa de seleção **Tamanho máximo de arquivo**. No campo à direita da caixa de seleção **Tamanho máximo de arquivo**, especifique o tamanho máximo do arquivo de relatório.

     Por padrão, o tamanho máximo do arquivo de relatório está limitado a 1024 MB.

   - Para remover a restrição do tamanho do arquivo de relatório, desmarque a caixa de seleção **Tamanho máximo de arquivo**.

   O limite do tamanho do arquivo de relatório está ativado por padrão.

4. Para salvar as alterações, clique no botão **Salvar**.

Visualize relatórios

Para visualizar relatórios:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Relatórios** para abrir a janela **Relatórios**.
3. Para gerar o relatório Todos os componentes de proteção, na parte esquerda da janela **Relatórios**, selecione o item **Todos os componentes de proteção** na lista de componentes e tarefas.

   O relatório Todos os componentes de proteção é exibido na parte direita da janela, que contém a lista de eventos no processamento de todos os componentes do Kaspersky Endpoint Security.

4. Para gerar um relatório de funcionamento de um componente ou tarefa, na parte esquerda da janela **Relatórios**, na lista de componentes e tarefas, selecione um componente ou tarefa.

Na parte direita da janela é exibido um relatório que contém uma lista de eventos do processamento do componente ou tarefa especificados do Kaspersky Endpoint Security.

Por padrão, os eventos do relatório são classificados na ordem ascendente de valores na coluna **Data do evento**.

Visualizar informações sobre o evento no relatório

Você pode visualizar um resumo detalhado de cada evento no relatório.

Para visualizar um resumo detalhado de um evento no relatório:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Relatórios** para abrir a janela **Relatórios**.
3. Na parte esquerda da janela, selecione o relatório relevante sobre o componente ou tarefa.

   Eventos incluídos no escopo do relatório são exibidos na tabela na parte direita da janela. Para encontrar eventos específicos no relatório, utilize as funções de filtro, pesquisa e classificação.
4. Selecione o evento relevante no relatório.

Uma seção com o resumo do evento é exibida na parte inferior da janela.

Salvar um relatório em arquivo

Você pode salvar o relatório gerado em um arquivo em formato de texto (TXT) ou em um arquivo CSV.

O Kaspersky Endpoint Security registra os eventos no relatório, na forma em que são exibidos na tela, ou seja, com as mesmas combinações e sequências dos atributos do evento.

Para salvar um relatório em arquivo:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Relatórios** para abrir a janela **Relatórios**.
3. Execute uma das seguintes ações:

   - Para gerar o relatório Todos os componentes de proteção, marque **Todos os componentes de proteção** na lista de componentes e tarefas.

     O relatório "Todos os componentes de proteção" é exibido na parte direita da janela e contém uma lista de eventos do processamento de todos os componentes de proteção.

   - Para gerar um relatório do processamento de um componente ou tarefa específicos, selecione-o na lista de componentes e tarefas.

     Na parte direita da janela é exibido um relatório que contém uma lista de eventos do processamento do componente ou tarefa especificado.
4. Se necessário, é possível modificar a apresentação de dados no relatório por meio de:

- Filtragem de eventos
- Execução de busca de evento
- Reordenação de colunas
- Classificação de eventos

5. Clique no botão **Salvar relatório** no canto superior direito da janela.

   É aberto um menu de contexto.

6. No menu de contexto, selecione a codificação desejada para salvar o arquivo: **Salvar como ANSI** ou **Salvar como Unicode**.

   A janela **Salvar como**, no Microsoft Office, é exibida.

7. Na janela **Salvar como**, especifique a pasta de destino do arquivo de relatório.
8. No campo **Nome do arquivo**, digite o nome do arquivo de relatório.
9. No campo **Tipo de arquivo**, selecione o formato desejado do relatório: TXT ou CSV.
10. Clique no botão **Salvar**.

Limpando relatórios

Para excluir informações dos relatórios:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Configurações Avançadas**, selecione **Relatórios e armazenamentos**.
3. Na parte direita da janela, na seção **Parâmetros do relatório**, clique no botão **Excluir relatórios**.

   A janela **Limpando relatórios** é aberta.

4. Marque as caixas de seleção ao lado dos relatórios que contêm as informações que deseja excluir:

   - **Todos os relatórios**.
   - **Relatório de proteção geral**. Contém informações sobre o funcionamento dos seguintes componentes do Kaspersky Endpoint Security:
     - Antivírus de Arquivos
     - Antivírus de e-mail.
     - Antivírus da Web.
     - Antivírus de MI.
     - Inspetor do Sistema.
     - Firewall.

- Bloqueio de Ataque de Rede.
- Prevenção contra ataque BadUSB.

- **Relatório de tarefas de verificação**. Contém informações sobre o processamento das tarefas de verificação:
  - Verificação completa
  - Verificação de Áreas Críticas
  - Verificação Personalizada
  - Verificação da integridade.
- **Relatório de tarefas de atualização**. Contém informações sobre o processamento das tarefas de atualização:
- **Relatório de firewall**. Contém informações sobre o processamento do Firewall.
- **Relatório dos componentes de controle**. Contém informações sobre o funcionamento dos seguintes componentes do Kaspersky Endpoint Security:
  - Controle de Inicialização de Aplicativo.
  - Controle de Privilégios de Aplicativo.
  - Monitoramento de Vulnerabilidades.
  - Controle de Dispositivo.
  - Controle da Web.
- **Relatório de criptografia de dados**.

5. Clique em **OK**.

Serviço de notificações

Esta seção fornece informações sobre o serviço de notificação que alerta o usuário sobre os eventos na operação do Kaspersky Endpoint Security, e também contém instruções sobre a configuração dos parâmetros de notificações.

Sobre as notificações do Kaspersky Endpoint Security

Vários tipos de eventos ocorrem durante a operação do Kaspersky Endpoint Security. As Notificações destes eventos podem ser puramente informativas ou conter informações importantes. Por exemplo, as notificações podem informar sobre atualização bem-sucedido do módulo de um aplicativo e de um banco de dados ou registrar erros de componentes que precisam ser corrigidos.

O Kaspersky Endpoint Security dá suporte ao registo de informações sobre eventos na operação do registro do aplicativo do Microsoft Windows e/ou do registro de eventos do Kaspersky Endpoint Security.

O Kaspersky Endpoint Security transmite as notificações das seguintes formas:

- usando notificações pop-up na área de notificação da barra de tarefas do Microsoft Windows;
- por e-mail.

Você pode configurar a transmissão de notificações de eventos. O método de transmissão de notificações é configurado para cada tipo de evento.

Configurar o serviço de notificações

Você pode executar as seguintes ações para configurar o serviço de notificação:

- Defina as configurações de registro de eventos onde o Kaspersky Endpoint Security registra eventos.
- Configure como as notificações são exibidas na tela.
- Configure a transmissão de notificações por e-mail.

Usando a tabela de eventos para configurar o serviço de notificação, você pode executar as seguintes ações:

- Filtre o serviço de notificações por valores da coluna ou por condições de filtragem personalizadas.
- Utilize a função de busca para eventos do serviço de notificações.
- Classifique os eventos do serviço de notificações.
- Altere a ordem e a configuração das colunas que são exibidas na lista de eventos do serviço de notificações.

Definir as configurações do registro de eventos

Para definir as configurações do registro de eventos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Configurações Avançadas**, selecione **Relatórios e armazenamentos**.

   A parte direita da janela exibe as configurações dos relatórios e do armazenamento.
3. Na seção **Notificações**, clique no botão **Configurações**.

   É exibida a janela **Notificações**.

   Os componentes e as tarefas do Kaspersky Endpoint Security são exibidos na parte esquerda da janela. A parte direita da janela lista os eventos gerados para o componente ou a tarefa selecionados.
4. Na parte esquerda da janela, selecione o componente ou a tarefa para os quais deseja definir as configurações do registro de eventos.
5. Marque as caixas de seleção ao lado dos eventos relevantes nas colunas **Salvar no registro local** e **Salvar no Registro de Evento do Windows**.

   Os eventos cujas caixas de seleção são marcadas na coluna **Salvar no registro local** são exibidos em **Registros de aplicativos e serviços** na seção **Kaspersky Event Log**. Os eventos cujas caixas de seleção são marcadas na coluna **Salvar no Registro de Evento do Windows** são exibidos nos **Logs do Windows** na seção **Aplicativo**. Para abrir os registros de eventos, clique em **Iniciar** → **Painel de comando** → **Administração** → **Visualizador de Eventos**.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Configurar a exibição e entrega de notificações

Para configurar a exibição e entrega de notificações:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Configurações Avançadas**, selecione **Relatórios e armazenamentos**.

   A parte direita da janela exibe as configurações dos relatórios e do armazenamento.
3. Na seção **Notificações**, clique no botão **Configurações**.

   É exibida a janela **Notificações**.

   Os componentes e as tarefas do Kaspersky Endpoint Security são exibidos na parte esquerda da janela. A parte direita da janela lista os eventos gerados para o componente ou a tarefa selecionada.
4. Na parte esquerda da janela, selecione o componente ou a tarefa para os quais deseja configurar a transmissão de notificações.
5. Na coluna **Notificar na tela**, marque as caixas de seleção ao lado dos eventos desejados.

   As informações sobre os eventos selecionados são exibidas na tela em mensagens pop-up na área de notificação da barra de tarefas do Microsoft Windows.
6. Na coluna **Notificar por e-mail**, marque as caixas de seleção ao lado dos eventos desejados.

   As informações sobre os eventos selecionados são entregues pelo e-mail se as configurações de entrega de notificação de correio forem configuradas.
7. Clique no botão **Configurações de notificação por e-mail**.

É exibida a janela **Configurações de notificação por e-mail**.

8. Marque a caixa de seleção **Enviar notificações de evento** para ativar a transmissão de informações de eventos do Kaspersky Endpoint Security selecionados na coluna **Notificar por e-mail**.

9. Especifique as configurações de transmissão de notificação por e-mail.

10. Clique em **OK**.

11. Na janela **Configurações de notificação por e-mail**, clique em **OK**.

12. Para salvar as alterações, clique no botão **Salvar**.

Configurar a exibição de avisos sobre o status do aplicativo na área de notificação

Para configurar a exibição de avisos de status do aplicativo na área de notificação:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, na seção **Configurações Avançadas**, selecione **Interface**.

   As configurações da interface do Kaspersky Endpoint Security são exibidas na parte direita da janela.

3. Na seção **Avisos**, marque as caixas de seleção ao lado das categorias de eventos sobre os quais você quer ver notificações na área de notificação do Microsoft Windows.

4. Para salvar as alterações, clique no botão **Salvar**.

Quando os eventos associados às categorias selecionadas ocorrerem, o ícone de aplicativo na área de notificação vai se modificar para ou , dependendo da gravidade do aviso.

Gerenciar a Quarentena e Backup

Esta seção descreve como configurar e gerenciar a Quarentena e Backup.

Sobre a Quarentena e Backup

A *Quarentena* é uma lista de arquivos provavelmente infectados. *Arquivos provavelmente infectados* são arquivos que podem conter vírus e outras ameaças ou as suas variedades.

Quando o Kaspersky Endpoint Security coloca um arquivo provavelmente infectado em quarentena, ele não faz uma cópia do arquivo, mas move-o de lugar: o aplicativo exclui o arquivo do disco rígido ou da mensagem de e-mail e o salva em um dispositivo de armazenamento de dados especial. Os arquivos em Quarentena são salvos em um formato especial e não representam uma ameaça.

O Kaspersky Endpoint Security pode detectar e isolar em quarentena um arquivo provavelmente infectado executando uma verificação de vírus e também durante a operação dos componentes Antivírus de Arquivos, Antivírus de E-mail e Inspetor do Sistema.

O Kaspersky Endpoint Security move arquivos para a Quarentena nos seguintes casos:

- O código do arquivo em análise é semelhante a um programa malicioso conhecido mas está parcialmente modificado, ou tem uma estrutura semelhante à de malware e não está registrado no banco de dados do Kaspersky Endpoint Security. Nesse caso, o arquivo é colocado em Quarentena após a execução da análise heurística pelo Antivírus de Arquivos e Antivírus de E-mail, ou durante uma verificação de vírus. A análise heurística raramente gera falsos positivos.

- A sequência de operações executadas pelo arquivo é perigosa. Nesse caso, o arquivo é colocado em quarentena após o componente Inspetor do Sistema analisar o comportamento deste.

O *backup* é uma lista de cópias de backup de arquivos que foram excluídos ou modificados durante o processo de desinfecção. A *cópia de backup* é uma cópia do arquivo criada na primeira tentativa de desinfecção ou exclusão deste arquivo. As cópias de backup de arquivos são armazenadas em um formato especial e não representam uma ameaça.

Em alguns casos não é possível manter a integridade de arquivos durante a desinfecção. Se após a desinfecção você perder o acesso parcial ou totalmente as informações importantes do arquivo desinfectado, é possível fazer uma tentativa de restaurar a cópia desinfectada do arquivo para a pasta de origem.

É possível que, após ser realizada uma nova atualização do banco de dados e dos módulos do software aplicativo, o Kaspersky Endpoint Security possa definitivamente identificar as ameaças e as neutralizar. Portanto, é recomendável verificar os arquivos em quarentena após cada atualização do banco de dados e dos módulos do software aplicativo.

Definir as configurações de Quarentena e Backup

O armazenamento de dados é composto por Quarentena e Backup. Você pode definir as configurações de Quarentena e Backup da seguinte forma:

- Configure o período máximo de armazenamento de arquivos na Quarentena e de cópias de arquivos no Backup.

O período máximo de trinta dias é o padrão para o armazenamento de arquivos na Quarentena e de cópias de arquivos no Backup. Quando o período máximo expira, o Kaspersky Endpoint Security exclui os arquivos mais antigos do armazenamento de dados. Você pode cancelar a restrição de tempo ou alterar a período máximo de armazenamento.

- É possível configurar a dimensão máxima de Quarentena e Backup

  Por padrão, a dimensão máxima de armazenamento em Quarentena e Backup é 100 MB. Quando for atingida a dimensão máxima de armazenamento de dados, o Kaspersky Endpoint Security exclui os arquivos mais antigos do armazenamento de Quarentena e Backup automaticamente para que o limite de armazenamento de dados máximo não seja excedido. É possível cancelar ou alterar o limite de tamanho de Quarentena e Backup.

Configurar o período máximo de armazenamento de arquivos na Quarentena e de cópias de arquivos no Backup

Para configurar o período máximo de armazenamento de arquivos na Quarentena e de cópias de arquivos no Backup:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Configurações Avançadas**, selecione **Relatórios e armazenamentos**.
3. Execute uma das seguintes ações:
   - Para limitar o período de armazenamento de arquivos na Quarentena e no Backup, na parte direita da janela na seção **Configurações de Quarentena e Backup**, marque a caixa de seleção **Armazenar objetos por no máximo**. No campo à direita da caixa de seleção **Armazenar objetos por no máximo**, especifique o período máximo de armazenamento de arquivos na Quarentena e de cópias de arquivos no Backup. O período de trinta dias é o padrão para o armazenamento de arquivos na Quarentena e de cópias de arquivos no Backup.
   - Para cancelar a limitação do período de armazenamento de arquivos na Quarentena e no Backup, na parte direita da janela na seção **Configurações de Quarentena e Backup**, marque a caixa de seleção **Armazenar objetos por no máximo**.
4. Para salvar as alterações, clique no botão **Salvar**.

Configurar a dimensão máxima de Quarentena e Backup

Para configurar o tamanho máximo de Quarentena e Backup:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Configurações Avançadas**, selecione **Relatórios e armazenamentos**.
3. Execute uma das seguintes ações:
   - Se desejar limitar o tamanho total da Quarentena e Backup, marque a caixa de seleção **Tamanho máximo de armazenamento**, na parte direita da janela na seção **Configurações de Quarentena e Backup**, e especifique o tamanho máximo da Quarentena e Backup no campo à direita da caixa de seleção **Tamanho máximo de armazenamento**.

Por padrão, o tamanho máximo do armazenamento de dados que compreende o diretório Quarentena e as cópias de backup de arquivos é de 100 MB.

- Se desejar remover o limite de tamanho da Quarentena e Backup, desmarque a caixa **Tamanho máximo de armazenamento**, na parte direita da janela, na seção **Configurações de Quarentena e Backup**.

O tamanho da Quarentena e Backup é ilimitado por padrão.

4. Para salvar as alterações, clique no botão **Salvar**.

Gerenciar a Quarentena

O Kaspersky Endpoint Security exclui automaticamente arquivos com qualquer status de Quarentena após a expiração do período de armazenamento definido nas configurações do aplicativo.

As seguintes operações nos arquivos estão disponíveis no gerenciamento da Quarentena:

- Exibir os arquivos colocados em quarentena pelo Kaspersky Endpoint Security.
- Verificar arquivos provavelmente infectados usando a versão atual dos bancos de dados e módulos do Kaspersky Endpoint Security.
- Restaurar arquivos da Quarentena e colocá-los na pasta de origem.
- Remover arquivos da Quarentena.
- Abrir as pastas em que os arquivos estavam originalmente.

O conjunto de arquivos em quarentena é apresentado como uma tabela.

Também é possível efetuar as seguintes ações ao gerenciar dados na tabela:

- Filtrar arquivos em Quarentena com base em colunas e condições de filtro personalizadas.
- Usar a função de busca de arquivo em quarentena.
- Classificar os arquivos em quarentena.
- Alterar a ordem e a configuração das colunas que são exibidas na tabela de arquivos em quarentena.

É possível copiar os eventos de quarentena selecionados para a área de transferência. Para selecionar múltiplos arquivos isolados em quarentena, clique com o botão direito do mouse para abrir o menu de contexto de qualquer arquivo e escolha **Selec. tudo**. Para desmarcar arquivos que você não quer verificar, clique neles enquanto pressiona a tecla **CTRL**.

Ativar e desativar a verificação de arquivos em Quarentena após atualização

Quando o Kaspersky Endpoint Security detecta sinais de infecção ao verificar um arquivo, mas não consegue identificar que programas maliciosos específicos a causaram, o Kaspersky Endpoint Security move este arquivo para a Quarentena. É possível que o Kaspersky Endpoint Security identifique as ameaças definitivamente e as neutralize quando realizar a atualização dos bancos de dados e dos módulos do aplicativo. Você pode configurar o início automático da verificação de arquivos em quarentena após realizar a atualização dos bancos de dados e dos módulos do aplicativo.

É recomendável fazer a verificação de arquivos em Quarentena regularmente. A verificação pode alterar o status dos arquivos. Dessa forma, alguns arquivos podem ser desinfectados e restaurados aos locais de origem, sendo permitido seu uso novamente.

Para ativar a verificação de arquivos em quarentena após realizar a atualização:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Configurações Avançadas**, selecione **Relatórios e armazenamentos**.

   Na parte direita da janela, as configurações de gerenciamento de relatórios e armazenamentos são exibidas.
3. Na seção **Configurações de Quarentena e Backup**, execute uma das seguintes ações:

   - Para ativar a verificação de arquivos em quarentena após realizar a atualização do Kaspersky Endpoint Security, marque a caixa de seleção **Verificar a Quarentena novamente após a atualização**.
   - Para desativar a verificação de arquivos em quarentena após realizar a atualização do Kaspersky Endpoint Security, desmarque a caixa de seleção **Verificar a Quarentena novamente após a atualização**.
4. Para salvar as alterações, clique no botão **Salvar**.

Executar uma tarefa de Verificação Personalizada para arquivos em quarentena

Após uma atualização dos bancos de dados e dos módulos de software do aplicativo, o Kaspersky Endpoint Security pode identificar definitivamente as ameaças de arquivos em Quarentena e neutralizá-los. Se o aplicativo não estiver configurado para verificar os arquivos em quarentena automaticamente após cada atualização dos bancos de dados e dos módulos do aplicativo, será possível executar a tarefa de Verificação Personalizada para arquivos em quarentena manualmente.

Para executar a tarefa de Verificação Personalizada para arquivos em quarentena:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.

   A guia **Quarentena** da janela **Armazenamentos** é exibida.
3. Na guia **Quarentena**, selecione um ou mais arquivos provavelmente infectados que deseja verificar.

   Para selecionar múltiplos arquivos isolados em quarentena, clique com o botão direito do mouse para abrir o menu de contexto de qualquer arquivo e escolha **Selec. tudo**. Para desmarcar arquivos que você não quer verificar, clique neles enquanto pressiona a tecla **CTRL**.
4. Inicie a tarefa de Verificação Personalizada da seguinte forma:

   - Clique no botão **Verificar novamente**.

- Clique com o botão direito do mouse para exibir o menu de contexto e selecione **Verificar novamente**.

Quando a verificação for concluída, aparece uma notificação que exibe a quantidade de arquivos verificados e de ameaças detectadas.

Restaurar arquivos da Quarentena

Para restaurar arquivos da quarentena:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.

   A guia **Quarentena** da janela **Armazenamentos** é exibida.
3. Se desejar restaurar todos os arquivos isolados em quarentena, selecione **Restaurar tudo** no menu de contexto de qualquer arquivo.

   O Kaspersky Endpoint Security restaura todos os arquivos da Quarentena para as respectivas pastas de origem.
4. Para restaurar um ou mais arquivos em quarentena:

   a. Na guia **Quarentena**, selecione um ou mais os arquivos que deseja restaurar da quarentena.

   Para selecionar múltiplos arquivos isolados em quarentena, clique com o botão direito do mouse para abrir o menu de contexto de qualquer arquivo e escolha **Selec. tudo**. Para desmarcar arquivos que você não quer verificar, clique neles enquanto pressiona a tecla **CTRL**.

   b. Restaure arquivos das seguintes formas:

   - Clique no botão **Restaurar**.
   - Clique com o botão direito do mouse para abrir o menu de contexto e selecione **Restaurar**.

O Kaspersky Endpoint Security restaura os arquivos selecionados para as respectivas pastas de origem.

Excluir arquivos da Quarentena

Para excluir arquivos da Quarentena:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.

   A guia **Quarentena** da janela **Armazenamentos** é exibida.
3. Se desejar excluir todos os arquivos da Quarentena, selecione **Excluir tudo** no menu de contexto de qualquer arquivo.

   O Kaspersky Endpoint Security exclui todos os arquivos selecionados da Quarentena.
4. Para excluir um ou mais arquivos em quarentena:

a. Na tabela da guia **Quarentena**, selecione um ou mais arquivos provavelmente infectados que deseja excluir da Quarentena.

Para selecionar múltiplos arquivos isolados em quarentena, clique com o botão direito do mouse para abrir o menu de contexto de qualquer arquivo e escolha **Selec. tudo**. Para desmarcar arquivos que você não quer verificar, clique neles enquanto pressiona a tecla **CTRL**.

b. Exclua arquivos das seguintes formas:

- Clique no botão **Remover**.
- Clique com o botão direito para abrir o menu de contexto e selecione **Excluir**.

O Kaspersky Endpoint Security exclui os arquivos selecionados da Quarentena.

Gerenciar o Backup

Se um código malicioso for detectado no arquivo, o Kaspersky Endpoint Security bloqueia o arquivo, coloca a sua cópia em Backup e tenta desinfectá-lo. Se a desinfecção for bem-sucedida, o status da cópia de backup do arquivo será alterado para *Desinfectado*. O arquivo fica disponível na sua pasta original. Se um arquivo não puder ser desinfectado, o Kaspersky Endpoint Security o exclui da sua pasta original. É possível restaurar o arquivo da cópia de backup para a respectiva pasta de origem.

Ao detectar código malicioso em um arquivo que faça parte do aplicativo Windows Store, o Kaspersky Endpoint Security exclui imediatamente o arquivo sem mover uma cópia dele para Backup. Você pode restaurar a integridade do aplicativo Windows Store usando as ferramentas adequadas do sistema operacional Microsoft Windows 8 (consulte os *arquivos de ajuda do Microsoft Windows 8* para obter detalhes sobre a restauração do aplicativo Windows Store).

O Kaspersky Endpoint Security exclui automaticamente as cópias de arquivos de backup com qualquer status de Backup após a expiração do período de armazenamento definido nas configurações do aplicativo.

Também é possível excluir manualmente qualquer cópia de um arquivo do Backup.

O conjunto de cópias de backup de arquivos é apresentado como uma tabela.

Ao gerenciar o Backup, você pode executar as seguintes operações com as cópias de backup dos arquivos:

- Exibir o conjunto de cópias de backup de arquivos.
- Restaurar arquivos das cópias de backup para as respectivas pastas de origem.
- Excluir cópias de backup de arquivos do Backup.

Também é possível efetuar as seguintes ações ao gerenciar dados na tabela:

- Filtrar cópias de backup por colunas, inclusive por condições de filtragem personalizadas.
- Usar a função de busca de cópias de backup.
- Classificar as cópias de backup.
- Alterar a ordem e a configuração das colunas que são exibidas na tabela de cópias de backup.

É possível copiar os eventos de backup selecionados para a área de transferência. Para selecionar múltiplos arquivos de Backup, clique com o botão direito do mouse para abrir o menu de contexto de qualquer arquivo e escolha **Selec. tudo**. Para desmarcar arquivos que você não quer verificar, clique neles enquanto pressiona a tecla **CTRL**.

Restaurar arquivos do Backup

Para restaurar arquivos do Backup:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.
3. Na janela **Armazenamentos**, selecione a guia **Backup**.
4. Se desejar restaurar todos os arquivos do Backup, selecione **Restaurar tudo** no menu de contexto de qualquer arquivo.

   O Kaspersky Endpoint Security restaura todos os arquivos das cópias de backup para as respectivas pastas de origem.
5. Para restaurar um ou mais arquivo do Backup:

   a. Na tabela da guia **Backup**, selecione um ou mais arquivos de Backup.

   Para selecionar múltiplos arquivos isolados em quarentena, clique com o botão direito do mouse para abrir o menu de contexto de qualquer arquivo e escolha **Selec. tudo**. Para desmarcar arquivos que você não quer verificar, clique neles enquanto pressiona a tecla **CTRL**.

   b. Restaure arquivos das seguintes formas:

   - Clique no botão **Restaurar**.
   - Clique com o botão direito do mouse para abrir o menu de contexto e selecione **Restaurar**.

   O Kaspersky Endpoint Security restaura os arquivos das cópias de backup selecionadas para as respectivas pastas de origem.

Excluir cópias de backup de arquivos do Backup

Para excluir cópias backup de arquivos do Backup:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela principal do aplicativo, clique no link **Quarentena** para abrir a janela **Armazenamentos**.
3. Na janela **Armazenamentos**, selecione a guia **Backup**.
4. Se você quiser apagar todos os arquivos do Backup, execute uma das seguintes ações:

- No menu de contexto de qualquer arquivo, selecione **Excluir tudo**.
- Clique no botão **Limpar armazenamento**.

O Kaspersky Endpoint Security exclui todas as cópias de backup dos arquivos do Backup.

5. Se desejar excluir um ou vários arquivos do Backup:

   a. Na tabela da guia **Backup**, selecione um ou mais arquivos de Backup.

   Para selecionar múltiplos arquivos de Backup, clique com o botão direito do mouse para abrir o menu de contexto de qualquer arquivo e escolha **Selec. tudo**. Para desmarcar arquivos que você não quer verificar, clique neles enquanto pressiona a tecla **CTRL**.

   b. Exclua arquivos das seguintes formas:

   - Clique no botão **Remover**.
   - Clique com o botão direito para abrir o menu de contexto e selecione **Excluir**.

O Kaspersky Endpoint Security exclui as cópias de backup dos arquivos selecionados do Backup.

Configurações avançadas do aplicativo

Esta seção descreve as configurações avançadas do Kaspersky Endpoint Security e contém informações sobre como defini-las.

Criar e usar um arquivo de configuração

Um arquivo de configuração com configurações do Kaspersky Endpoint Security permite que você realize as seguintes tarefas:

- Executar a instalação local do Kaspersky Endpoint Security via linha de comando com configurações predefinidas.

  Para fazer assim, você deve salvar o arquivo de configuração na mesma pasta em que o kit de distribuição está localizado.

- Executar a instalação remota do Kaspersky Endpoint Security via Kaspersky Security Center com configurações predefinidas.

- Migrar configurações do Kaspersky Endpoint Security de um computador ao outro.

Para criar o arquivo de configuração:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.

   As configurações avançadas do aplicativo são exibidas na parte direita da janela.
3. Na seção **Gerenciar configurações**, clique no botão **Salvar**.

   É exibida a janela padrão do Microsoft Windows **Selecionar um arquivo de configuração**.
4. Especifique o caminho no qual você quer salvar o arquivo de configuração e digite o seu nome.

   Para usar o arquivo de configuração para a instalação local ou remota do Kaspersky Endpoint Security, você deve denominá-lo install.cfg.
5. Clique no botão **Salvar**.

Para importar configurações do Kaspersky Endpoint Security de um arquivo de configuração:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.

   As configurações avançadas do aplicativo são exibidas na parte direita da janela.
3. Na seção **Gerenciar configurações**, clique no botão **Carregar**.

   É exibida a janela padrão do Microsoft Windows **Selecionar um arquivo de configuração**.
4. Especifique o caminho para o arquivo de configuração.
5. Clique no botão **Abrir**.

Todos os valores das configurações do Kaspersky Endpoint Security serão definidos de acordo com o arquivo de configuração selecionado.

Zona confiável

Esta seção contém informações sobre a zona confiável e as instruções para configurar a exclusão de verificação e criar um lista de aplicativos confiáveis.

Sobre a zona confiável

A *zona confiável* é uma lista de objetos e aplicativos configuradas pelo administrador de sistema que o Kaspersky Endpoint Security não monitora quando ativado. Por outras palavras, é um conjunto de exclusões de verificação.

O administrador cria a zona confiável individualmente, considerando as características dos objetos processados e dos aplicativos que estão instalados no computador. Talvez seja necessário incluir objetos e aplicativos na zona confiável se o Kaspersky Endpoint Security bloquear o acesso a um objeto ou aplicativo determinado, quando você tem certeza de que ele é inofensivo.

Você pode excluir os seguintes objetos da verificação:

- Arquivos de determinados formatos
- Arquivos selecionados por uma máscara
- Arquivos selecionados
- Pastas
- Processos de aplicativos

Exclusões de verificação

A *exclusão de verificação* é um conjunto de condições segundo as quais o Kaspersky Endpoint Security não verifica um objeto para detectar vírus ou outras ameaças.

As exclusões de verificação tornam possível usar em segurança software legítimo que pode ser explorado por criminosos para danificar o computador ou os dados do usuário. Embora não tenham nenhuma atividade maliciosa, esses aplicativos podem ser usados como um componente auxiliar de malware. Exemplos de aplicativos incluem ferramentas de administração remota, clientes IRC, servidores FTP, vários utilitários que interrompem ou ocultam processos, keyloggers, violadores de senha e discadores automáticos. Tais aplicativos não são categorizados como vírus. Informações sobre softwares legais que podem ser utilizados por criminosos para danificar seu computador ou dados pessoais estão disponíveis no site da Enciclopédia de vírus da Kaspersky em https://encyclopedia.kaspersky.com/knowledge/riskware/.

Estes aplicativos poderão ser bloqueados pelo Kaspersky Endpoint Security. Para impedir que eles sejam bloqueados, você pode configurar exclusões de verificação para os aplicativos em uso. Para fazer isso, adicione o nome ou o nome da máscara que está listada na Enciclopédia de vírus da Kaspersky à zona confiável. Por exemplo, talvez você use com frequência o programa Administração remota. Este é um aplicativo de acesso remoto que permite o controle sobre um computador remoto. O Kaspersky Endpoint Security considera esta atividade como suspeita e poderá bloqueá-la. Para evitar que o aplicativo seja bloqueado, crie uma exclusão de verificação com o nome ou máscara de nome listado na Enciclopédia de vírus da Kaspersky.

Se um aplicativo que reúne informações e as envia para serem processadas for instalado no seu computador, o Kaspersky Endpoint Security pode classificar este aplicativo como malware. Para evitar isto, você pode excluir o aplicativo da verificação configurando o Kaspersky Endpoint Security como descrito neste documento.

Exclusões de verificação são usadas pelos seguintes componentes e tarefas do aplicativo que são configurados pelo administrador do sistema:

- Antivírus de Arquivos
- Antivírus de e-mail.
- Antivírus da Web.
- Controle de Privilégios de Aplicativo.
- Tarefas de verificação
- Inspetor do Sistema.

Lista de aplicativos confiáveis

A *lista de aplicativos confiáveis* é uma lista de aplicativos cuja atividade de arquivo e rede (inclusive atividade maliciosa) e acesso ao registro do sistema e que não são monitorados pelo Kaspersky Endpoint Security. Por padrão, o Kaspersky Endpoint Security verifica todos os objetos que são abertos, executados ou salvos por qualquer processo do programa e controla a atividade de todos os aplicativos e tráfego de rede criada por eles. O Kaspersky Endpoint Security exclui aplicativos na lista de aplicativos confiáveis na verificação.

Por exemplo, se considerar que os objetos usados pelo Bloco de Notas do Microsoft Windows são seguros, e que não precisam ser verificados, ou seja, se você confia nesse aplicativo, adicione o Bloco de Notas do Microsoft Windows à lista de aplicativos confiáveis. Dessa forma, a verificação ignorará os objetos usados por este aplicativo.

Além disso, algumas ações classificadas como suspeitas pelo Kaspersky Endpoint Security podem ser consideradas seguras por vários aplicativos. Por exemplo, a interceptação de dados digitados no teclado é um processo de rotina dos programas que alternam automaticamente o layout do teclado (como o Punto Switcher). Para considerar as especificidades desses aplicativos e desativar o monitoramento de suas atividades, é recomendável adicioná-los à lista de aplicativos confiáveis.

A exclusão de aplicativos confiáveis da verificação permite evitar problemas de compatibilidade entre o Kaspersky Endpoint Security e outros programas (por exemplo, a verificação duplicada do tráfego de rede de um computador de terceiros pelo Kaspersky Endpoint Security e por outro aplicativo de antivírus), além de melhorar o desempenho do computador, que é crítico ao usar aplicativos do servidor.

Ao mesmo tempo, o arquivo executável e o processo do aplicativo confiável são verificados para detectar vírus e outro tipo de malware. O aplicativo pode ser excluído completamente da verificação do Kaspersky Endpoint Security por meio das exclusões de verificação.

Criar uma exclusão de verificação

O Kaspersky Endpoint Security não verifica um objeto se a unidade ou a pasta que contém este objeto estiver incluída no escopo da verificação no início de uma das tarefas de verificação. Contudo, a exclusão de verificação não é aplicada na execução da tarefa de Verificação Personalizada deste objeto.

Para criar uma exclusão de verificação:

1. Abra a janela de configurações do aplicativo.

2. Selecione a seção **Proteção antivírus** à esquerda.

   As configurações da proteção antivírus são exibidas na parte direita da janela.

3. Na seção **Exclusões de verificação e aplicativos confiáveis**, clique no botão **Configurações**.

   A janela **Zona confiável** abre na guia **Exclusões de verificação**.

4. Clique no botão **Adicionar**.

   A janela **Exclusão de verificação** é exibida. Nessa janela, você pode criar uma exclusão de verificação usando um ou ambos critérios da seção **Propriedades**.

5. Para excluir um arquivo ou pasta da verificação:

   a. Na seção **Propriedades**, selecione a caixa de seleção **Arquivo ou pasta**.

   b. Clique no link **selecionar arquivo ou pasta** na seção **Descrição da exclusão de verificação** para abrir a janela **Nome do arquivo ou pasta**.

   c. Insira o nome do arquivo ou da pasta ou a máscara do nome do arquivo ou da pasta ou selecione o arquivo ou a pasta na árvore da pasta clicando em **Procurar**.

   Em um arquivo ou máscara de nome da pasta, você pode usar o caráter de asterisco (*) para tomar o lugar de qualquer conjunto de caracteres no nome de arquivo.

   Por exemplo, você pode usar máscaras para adicionar os seguintes caminhos:

   - Caminhos a arquivos localizaram em qualquer pasta:
     - A máscara "*.exe" incluirá todos os caminhos para arquivos que com a extensão EXE.
     - A máscara "teste" incluirá todos os caminhos para arquivos nomeados "teste".
   - Caminhos a arquivos localizaram em uma pasta especificada:
     - A máscara "C:\dir*.*" incluirá todos os caminhos para arquivos localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
     - A máscara "C:\dir*" incluirá todos os caminhos para arquivos localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
     - A máscara "C:\dir\" incluirá todos os caminhos para arquivos localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
     - A máscara "C:\dir*.exe" incluirá todos os caminhos para arquivos com a extensão EXE localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
     - A máscara "C:\dir\test" incluirá todos os caminhos para arquivos nomeados "teste" localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
     - A máscara "C:\dir*\test" incluirá todos os caminhos para arquivos nomeados "teste" localizados na pasta C:\dir\ e nas subpastas de C:\dir\.
   - Caminhos para arquivos localizados em todas as pastas com um nome especificado:
     - A máscara "dir*.*" incluirá todos os caminhos para arquivos em pastas nomeadas "dir", mas não nas subpastas dessas pastas.

- A máscara "dir*" incluirá todos os caminhos para arquivos em pastas nomeadas "dir", mas não nas subpastas dessas pastas.
- A máscara "dir\" incluirá todos os caminhos para arquivos nas pastas denominadas "dir", mas não nas subpastas dessas pastas.
- A máscara "dir*.exe" incluirá todos os caminhos para arquivos com a extensão EXE em pastas nomeadas "dir", mas não nas subpastas dessas pastas.
- A máscara "dir\test" incluirá todos os caminhos para arquivos nomeados "teste" em pastas nomeadas "dir", mas não nas subpastas dessas pastas.

d. Na janela **Nome do arquivo ou pasta**, clique em **OK**.

Um link para o arquivo ou pasta adicionados é exibido na seção **Descrição da exclusão de verificação** da janela **Exclusão de verificação**.

6. Para excluir objetos com um nome específico da verificação:

a. Na seção **Propriedades**, selecione a caixa de seleção **Nome do objeto**.

b. Clique no link **inserir nome do objeto** na seção **Descrição da exclusão de verificação** para abrir a janela **Nome do objeto**.

c. Insira o nome ou a máscara do nome de acordo com a classificação da Enciclopédia de Vírus da Kaspersky:

d. Clique em **OK** na janela **Nome do objeto**.

Um link para o nome do objeto adicionado é exibido na seção **Descrição da exclusão de verificação** da janela **Exclusão de verificação**.

7. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

8. Especifique os componentes do Kaspersky Endpoint Security que devem usar a exclusão de verificação:

a. Clique no link **qualquer** na seção **Descrição da exclusão de verificação** para abrir o link **selecionar componentes**.

b. Clique no link **selecionar componentes** para abrir a janela **Componentes de proteção**.

c. Selecione as caixas em frente dos componentes aos quais a exclusão de verificação deve ser aplicada.

d. Na janela **Componentes de proteção**, clique em **OK**.

Se os componentes forem especificados nas configurações da exclusão de verificação, essa exclusão será aplicada apenas durante a verificação feita por esses componentes do Kaspersky Endpoint Security.

Se os componentes não forem especificados nas configurações da exclusão de verificação, esta exclusão será aplicada durante a verificação feita por todos os componentes do Kaspersky Endpoint Security.

9. Na janela **Exclusão de verificação**, clique em **OK**.

A exclusão de verificação que você adicionou é exibida na tabela da guia **Exclusões de verificação** da janela **Zona confiável**. As configurações especificadas para essa exclusão de verificação são exibidas na seção **Descrição da exclusão de verificação**.

10. Na janela **Zona confiável**, clique em **OK**.

11. Para salvar as alterações, clique no botão **Salvar**.

Modificar uma exclusão de verificação

Para modificar uma exclusão de verificação:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Proteção antivírus** à esquerda.

   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na seção **Exclusões de verificação e aplicativos confiáveis**, clique no botão **Configurações**.

   A janela **Zona confiável** abre na guia **Exclusões de verificação**.
4. Selecione a exclusão de verificação que você deseja modificar na lista.
5. Altere as configurações de exclusão de verificação usando um dos seguintes métodos:

   - Clique no botão **Editar**.

     A janela **Exclusões de verificação** é exibida.
   - Abra a janela para editar a definição necessária clicando no link no campo **Descrição da exclusão de verificação**.
6. Se tiver clicado no botão **Editar** na etapa anterior, clique em **OK** na janela **Exclusão de verificação**.

   As configurações modificadas para essa exclusão de verificação são exibidas na seção **Descrição da exclusão de verificação**.
7. Na janela **Zona confiável**, clique em **OK**.
8. Para salvar as alterações, clique no botão **Salvar**.

Excluir uma exclusão de verificação

Para excluir uma exclusão de verificação:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Proteção antivírus** à esquerda.

   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na seção **Exclusões de verificação e aplicativos confiáveis**, clique no botão **Configurações**.

   A janela **Zona confiável** abre na guia **Exclusões de verificação**.
4. Selecione a exclusão de verificação na lista de exclusões de verificação.
5. Clique no botão **Remover**.

   A exclusão de verificação excluída desaparece da lista.

6. Na janela **Zona confiável**, clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Ativar ou desativar uma exclusão de verificação

Para ativar ou desativar uma exclusão de verificação:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Proteção antivírus** à esquerda.
   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na seção **Exclusões de verificação e aplicativos confiáveis**, clique no botão **Configurações**.
   A janela **Zona confiável** abre na guia **Exclusões de verificação**.
4. Selecione a exclusão na lista de exclusões de verificação.
5. Execute uma das seguintes ações:
   - Para ativar uma exclusão de verificação, selecione a caixa de seleção junto do nome dessa exclusão de verificação.
   - Para desativar uma exclusão de verificação, desmarque a caixa de seleção junto do nome dessa exclusão de verificação.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Editar a lista de aplicativos confiáveis

Para editar a lista de aplicativos confiáveis:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Proteção antivírus** à esquerda.
   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na seção **Exclusões de verificação e aplicativos confiáveis**, clique no botão **Configurações**.
   A janela **Zona confiável** é exibida.
4. Na janela **Zona confiável**, selecione a guia **Aplicativos confiáveis**.
5. Para adicionar um aplicativo à lista de aplicativos confiáveis:
   a. Clique no botão **Adicionar**.
   b. No menu de contexto exibido, execute uma das seguintes operações:

- Se desejar encontrar o aplicativo na lista de aplicativos instalados no computador, selecione o item **Aplicativos** no menu.

  A janela **Selecionar aplicativo** é exibida.

- Se desejar especificar o caminho para o arquivo executável do aplicativo desejado, selecione **Procurar**.

  A janela padrão **Abrir arquivo**, no Microsoft Windows, é exibida.

c. Selecione o aplicativo de uma das seguintes formas:

- Se você tiver selecionado **Aplicativos** na etapa anterior, selecione o aplicativo na lista de aplicativos instalados no computador e clique em **OK** na janela **Selecionar aplicativo**.

- Se você tiver selecionado **Procurar** na etapa anterior, especifique o caminho do arquivo executável do aplicativo relevante e clique no botão **Abrir** na janela **Abrir** padrão do Microsoft Windows.

Essas ações fazem a janela **Exclusões de verificação para aplicativo** abrir.

a. Marque as caixas de seleção ao lado das regras da zona confiável relevantes para o aplicativo selecionado:

- **Não verificar arquivos abertos**.
- **Não monitorar a atividade de aplicativos**.
- **Não herdar restrições do processo principal (aplicativo)**.
- **Não monitorar a atividade de aplicativos secundários**.
- **Não bloquear interação com interface de aplicativo**.
- **Não verificar o tráfego de rede**.

b. Na janela **Exclusões de verificação para aplicativo**, clique em **OK**.

O aplicativo confiável adicionado aparece na lista de aplicativos confiáveis.

6. Para editar as configurações de um aplicativo confiável:

a. Selecione o aplicativo confiável na lista de aplicativos confiáveis.

b. Clique no botão **Editar**.

c. A janela **Exclusão de verificação de aplicativo** é exibida.

d. Marque ou desmarque as caixas de seleção ao lado das regras da zona confiável relevante do aplicativo selecionado:

> Se nenhuma regra da zona confiável for selecionada na janela **Exclusões de verificação para aplicativo**, o aplicativo confiável será incluído na verificação. Nesse caso, o aplicativo confiável não é removido da lista de aplicativos confiáveis, mas a caixa de seleção correspondente é desmarcada.

e. Na janela **Exclusões de verificação para aplicativo**, clique em **OK**.

7. Para remover um aplicativo confiável da lista de aplicativos confiáveis:

a. Selecione o aplicativo confiável na lista de aplicativos confiáveis.

b. Clique no botão **Remover**.

8. Na janela **Zona confiável**, clique em **OK**.
9. Para salvar as alterações, clique no botão **Salvar**.

Ativar e desativar regras da zona confiável para um aplicativo na lista de aplicativos confiáveis

Para ativar ou desativar a ação de regras da zona confiável aplicada a um aplicativo da lista de aplicativos confiáveis:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Proteção antivírus** à esquerda.

   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na seção **Exclusões de verificação e aplicativos confiáveis**, clique no botão **Configurações**.

   A janela **Zona confiável** é exibida.
4. Na janela **Zona confiável**, selecione a guia **Aplicativos confiáveis**.
5. Na lista de aplicativos confiáveis, selecione o aplicativo confiável desejado.
6. Execute uma das seguintes ações:

   - Para excluir um aplicativo confiável da verificação do Kaspersky Endpoint Security, marque a caixa de seleção próxima do nome deste.
   - Para incluir um aplicativo confiável na verificação do Kaspersky Endpoint Security, desmarque a caixa de seleção próxima do nome deste.
7. Clique em **OK**.
8. Para salvar as alterações, clique no botão **Salvar**.

Usar armazenamento de certificado de sistema confiável

O uso do armazenamento de certificado de sistema permite excluir aplicativos assinados por uma assinatura digital confiável de verificações de vírus. O Kaspersky Endpoint Security atribui automaticamente esses aplicativos ao grupo *Confiável*.

Para começar a usar o armazenamento de certificado de sistema confiável:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Proteção antivírus** à esquerda.

   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na seção **Exclusões de verificação e aplicativos confiáveis**, clique no botão **Configurações**.

A janela **Zona confiável** é exibida.

4. Na janela **Zona confiável**, selecione a guia **Armazenamento de certificado do sistema confiável**.
5. Marque a caixa de seleção **Usar armazenamento de certificado do sistema confiável**.
6. Na lista suspensa **Armazenamento de certificado do sistema confiável**, selecione qual armazenamento do sistema o Kaspersky Endpoint Security deve considerar como confiável.
7. Na janela **Zona confiável**, clique em **OK**.
8. Para salvar as alterações, clique no botão **Salvar**.

Autodefesa do Kaspersky Endpoint Security

Esta seção descreve os mecanismos de autodefesa e de proteção contra o controle externo do Kaspersky Endpoint Security e contém instruções para configurá-los.

Sobre a Autodefesa do Kaspersky Endpoint Security

O Kaspersky Endpoint Security oferece proteção ao computador contra programas maliciosos, incluindo tentativas de malware de bloquear as operações do aplicativo e inclusive excluí-lo do computador.

A Autodefesa, e os mecanismos de proteção contra o controle externo, do Kaspersky Endpoint Security, permitem a estabilidade do sistema de segurança no computador.

O mecanismo de *Autodefesa* impede que haja alteração, ou exclusão, de arquivos no disco rígido, processos na memória e entradas no registro do sistema.

A Proteção contra o controle externo bloqueia todas as tentativas de um computador remoto de controlar os serviços do aplicativo.

Em computadores que funcionam com sistemas operacionais de 64 bits, somente a Autodefesa do Kaspersky Endpoint Security está disponível para impedir a alteração e a exclusão de arquivos do aplicativo em entradas de disco rígido e registro de sistema.

Ativar ou desativar a Autodefesa

O mecanismo de Autodefesa do Kaspersky Endpoint Security está ativado por padrão. Se necessário, é possível desativar a Autodefesa.

Para ativar ou desativar a Autodefesa:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.

   As configurações avançadas do aplicativo são exibidas na parte direita da janela.

3. Execute uma das seguintes ações:

   - Para ativar o mecanismo de Autodefesa, marque a caixa de seleção **Ativar a Autodefesa**.
   - Para desativar o mecanismo de Autodefesa, desmarque a caixa de seleção **Ativar a Autodefesa**.

4. Para salvar as alterações, clique no botão **Salvar**.

Ativar ou desativar a Proteção contra o controle externo

O mecanismo de proteção contra o controle externo está ativo por padrão. Se necessário, você pode desativar o mecanismo de proteção contra o controle externo.

Para ativar ou desativar o mecanismo de proteção contra o controle externo:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.

   As configurações avançadas do aplicativo são exibidas na parte direita da janela.

3. Execute uma das seguintes ações:

   - Para ativar o mecanismo de proteção contra o controle externo, selecione **Desativar o gerenciamento externo do serviço do sistema**.
   - Para desativar o mecanismo de proteção contra o controle externo, desmarque **Desativar o gerenciamento externo do serviço do sistema**.

4. Para salvar as alterações, clique no botão **Salvar**.

Suportar aplicativos de administração remota

Excepcionalmente, será necessário usar um programa de administração remota enquanto a proteção de controle externo estiver ativa.

Para ativar a execução de aplicativos de administração remota:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Proteção antivírus** à esquerda.

   As configurações da proteção antivírus são exibidas na parte direita da janela.

3. Na seção **Exclusões de verificação e aplicativos confiáveis**, clique no botão **Configurações**.

   A janela **Zona confiável** é exibida.

4. Na janela **Zona confiável**, selecione a guia **Aplicativos confiáveis**.
5. Clique no botão **Adicionar**.
6. No menu de contexto exibido, execute uma das seguintes operações:

- Para buscar o programa de administração remota na lista de aplicativos instalados no computador, selecione o item **Aplicativos**.

  A janela **Selecionar aplicativo** é exibida.

- Para especificar o caminho para o arquivo executável do programa de administração remota, selecione **Procurar**.

  A janela padrão **Abrir arquivo**, no Microsoft Windows, é exibida.

7. Selecione o aplicativo de uma das seguintes formas:

   - Se você tiver selecionado **Aplicativos** na etapa anterior, selecione o aplicativo na lista de aplicativos instalados no computador e clique em **OK** na janela **Selecionar aplicativo**.

   - Se você tiver selecionado **Procurar** na etapa anterior, especifique o caminho do arquivo executável do aplicativo relevante e clique no botão **Abrir** na janela **Abrir** padrão do Microsoft Windows.

   Essas ações fazem a janela **Exclusões de verificação para aplicativo** abrir.

8. Marque a caixa de seleção **Não monitorar a atividade de aplicativos**.

9. Na janela **Exclusões de verificação para aplicativo**, clique em **OK**.

   O aplicativo confiável adicionado aparece na lista de aplicativos confiáveis.

10. Para salvar as alterações, clique no botão **Salvar**.

Desempenho do Kaspersky Endpoint Security e compatibilidade com outros aplicativos

Esta seção contém informações sobre desempenho do Kaspersky Endpoint Security e compatibilidade com outros aplicativos e também orientações sobre a seleção dos tipos de objetos detectáveis e o modo de operação do Kaspersky Endpoint Security.

Sobre o Desempenho do Kaspersky Endpoint Security e a compatibilidade com outros aplicativos

Desempenho do Kaspersky Endpoint Security

O desempenho do Kaspersky Endpoint Security refere-se ao número de tipos de objeto que podem danificar o computador que são detectáveis, bem como o consumo de energia e de recursos do computador.

Selecionar tipos de objetos detectáveis

O Kaspersky Endpoint Security permite ajustar detalhadamente a proteção de seu computador e selecionar os tipos de objetos que o aplicativo detecta durante a operação. O Kaspersky Endpoint Security sempre verifica o sistema operacional para detectar vírus, worms e Cavalos de troia. Não é possível desativar a verificação de objetos desse tipo. Estes malware conseguem causar grandes danos ao computador. O aumento da segurança do computador é obtido com a expansão da gama de tipos de objetos , que podem ser detectados por meio do controle de softwares legais que podem ser usados por criminosos para danificar o computador ou os dados pessoais.

Usar o modo de economia de energia

No que diz respeito a laptops, o consumo de energia devido ao uso de aplicativos precisa ser levado em consideração. As tarefas agendadas do Kaspersky Endpoint Security geralmente utilizam uma grande quantidade de recursos. Quando o computador está ligado usando a bateria, você pode usar o modo de economia de energia para poupar esta.

No modo de economia de energia, as seguintes tarefas agendadas são adiadas automaticamente:

- Tarefa de Atualização
- Tarefa de Verificação Completa
- Tarefa de Verificação de Áreas Críticas
- Tarefa de Verificação Personalizada
- Tarefa de Verificação de Vulnerabilidades
- Tarefa de Verificação da Integridade

Quer o modo de economia de energia esteja ou não ativo, o Kaspersky Endpoint Security pausa as tarefas de criptografia quando um computador portátil alterna para a energia da bateria. O aplicativo continua as tarefas de criptografia quando o computador portátil alterna da energia da bateria para energia elétrica.

Conceder recursos a outros aplicativos

A utilização de recursos do computador pelo Kaspersky Internet Security pode afetar o desempenho de outros aplicativos. Para resolver o problema da operação simultânea durante um maior carregamento da CPU e de subsistemas do disco rígido, o Kaspersky Endpoint Security pode pausar tarefas planejadas e conceder mais recursos a outros aplicativos.

Contudo, há um número grande de aplicativos que são iniciados assim que os recursos da CPU estão disponíveis, sendo executados em segundo plano. Para evitar que a verificação dependa do desempenho de outros aplicativos, é melhor não conceder recursos do sistema operacional.

Estas tarefas podem ser iniciadas manualmente, se necessário.

Usar a tecnologia de desinfecção avançada

Os programas maliciosos atuais conseguem invadir os níveis mais baixos de um sistema operacional, o que torna praticamente impossível excluí-los. Depois de detectar atividade maliciosa no sistema operacional, o Kaspersky Endpoint Security executa um procedimento de desinfeção extenso que usa a tecnologia de desinfecção avançada especial. A *tecnologia de desinfecção avançada* objetiva eliminar do sistema operacional programas maliciosos que já iniciaram seus processos na RAM e que impedem que o Kaspersky Endpoint Security os remova, usando outros métodos. Como resultado, a ameaça é neutralizada. Enquanto a Desinfecção Avançada estiver em andamento, é recomendável abster-se de iniciar novos processos ou editar os registros do sistema operacional. A tecnologia de desinfecção avançada usa uma grande quantidade de recursos do sistema operacional, que talvez torne os outros aplicativos mais lentos.

Depois que o processo de Desinfecção avançada estiver concluído em um computador executando o Microsoft Windows para estações de trabalho, o Kaspersky Endpoint Security solicitará a permissão do usuário para reiniciar o computador. Após a reinicialização do sistema, o Kaspersky Endpoint Security exclui os arquivos de malware files e inicia uma verificação completa "leve" do computador.

A solicitação de reinicialização é impossível em computadores que executem o Microsoft Windows para servidores de arquivos devido às especificações do Kaspersky Endpoint Security para servidores de arquivos. Uma reinicialização não planejada de um servidor de arquivos pode gerar problemas envolvendo a indisponibilidade temporária dos dados do servidor ou perda de dados não salvos. É recomendável reiniciar um servidor de arquivos estritamente de acordo com o agendamento. É por isso que a Tecnologia de Desinfecção Avançada é desativada por padrão para servidores de arquivos.

Se uma infecção ativa for detectada em um servidor de arquivo, ela é retransmitida ao Kaspersky Security Center com a informação de que é necessária a desinfecção ativa. Para Desinfectar uma infecção ativa em um servidor de arquivos, ative a tecnologia de desinfecção ativa para os servidores de arquivos e inicie uma tarefa de grupo de *Verificação de vírus* em um horário conveniente para os usuários do servidor de arquivos.

Selecionar tipos de objetos detectáveis

Para selecionar os tipos objetos detectáveis:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção antivírus**.

   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na seção **Objetos**, clique no botão **Configurações**.

   A janela **Objetos para detecção** é exibida.
4. Marque as caixas de seleção em frente às ameaças que você deseja detectar com o Kaspersky Endpoint Security:

   - **Ferramentas maliciosas**
   - **Adware**
   - **Discadores automáticos**
   - **Outra**
   - **Arquivos compactados que podem causar danos**
   - **Arquivos multicompactados**
5. Clique em **OK**.

A janela **Objetos para detecção** fecha. Na seção **Objetos**, os tipos de objetos selecionados são apresentados em **A detecção dos seguintes tipos de objeto está ativada**.

6. Para salvar as alterações, clique no botão **Salvar**.

Ativar ou desativar a tecnologia de desinfecção avançada para estações de trabalho

Para ativar ou desativar a Tecnologia de desinfecção avançada:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção antivírus**.

   As configurações da proteção antivírus são exibidas na parte direita da janela.
3. Na parte direita da janela, execute uma das seguintes operações:
   - Marque **Ativar a Tecnologia de desinfecção avançada** para ativar a Tecnologia de desinfecção avançada.
   - Desmarque **Ativar a Tecnologia de desinfecção avançada** para desativar a Tecnologia de desinfecção avançada.
4. Para salvar as alterações, clique no botão **Salvar**.

Quando a tarefa de Desinfecção Avançada é iniciada através do Kaspersky Security Center, a maioria das funções do sistema operacional estão indisponíveis ao usuário. A estação de trabalho é reiniciada após a tarefa ter sido concluída.

Ativar ou desativar a tecnologia de desinfecção avançada para servidores de arquivo

Para ativar a Tecnologia de Desinfecção Avançada para servidores de arquivo, realize uma das seguintes operações:

- Ative a tecnologia de desinfecção avançada nas propriedades da política ativa do Kaspersky Security Center. Para fazer isso:
  a. Abra a seção **Configurações de Proteção Geral** na janela de propriedades da política.
  b. Marque a caixa de seleção **Ativar a Tecnologia de Desinfecção Avançada**.
  c. Para salvar as modificações, clique em **OK** na janela de propriedades da política.
- Nas propriedades da tarefa de grupo Verificação de vírus do Kaspersky Security Center, marque a caixa de seleção **Executar a Desinfecção Avançada imediatamente**.

Para desativar a tecnologia de desinfecção avançada para servidores de arquivo, execute uma das seguintes operações:

- Ative a tecnologia de desinfecção avançada nas propriedades da política do Kaspersky Security Center. Para fazer isso:

  a. Abra a seção **Configurações de Proteção Geral** na janela de propriedades da política.

  b. Desmarque a caixa de seleção **Ativar a Tecnologia de Desinfecção Avançada**.

  c. Para salvar as modificações, clique em **OK** na janela de propriedades da política.

- Nas propriedades da tarefa de grupo Verificação de vírus do Kaspersky Security Center, desmarque a caixa de seleção **Executar a Desinfecção Avançada imediatamente**.

Ativar ou desativar o modo de economia de energia

Para ativar ou desativar o modo de economia de energia:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.

   As configurações avançadas do aplicativo são exibidas na parte direita da janela.
3. Na seção **Modo operacional**, clique no botão **Configurações**.

   A janela **Modo operacional** é exibida.
4. Execute as seguintes ações na janela **Modo operacional**:

   - Para ativar o modo de economia de energia, marque a caixa de seleção **Adiar tarefas agendadas quando estiver em modo de bateria**.

     Quando o modo de conservação de energia é ativado e o computador estiver sendo executado no modo de energia da bateria, as seguintes tarefas não serão executadas mesmo se agendadas:

     - Tarefa de Atualização
     - Tarefa de Verificação Completa
     - Tarefa de Verificação de Áreas Críticas
     - Tarefa de Verificação Personalizada
     - Tarefa de Verificação de Vulnerabilidades
     - Tarefa de Verificação da Integridade

   - Se desejar desativar o modo de economia de energia, desmarque a caixa de seleção **Adiar tarefas agendadas quando estiver em modo de bateria**. Nesse caso, o Kaspersky Endpoint Security executa as tarefas agendadas independentemente da fonte de alimentação do computador.
5. Para salvar as alterações, clique no botão **Salvar**.

Ativar ou desativar a concessão de recursos a outros aplicativos

Para ativar ou desativar a concessão de recursos a outros aplicativos:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.

   As configurações avançadas do aplicativo são exibidas na parte direita da janela.
3. Na seção **Modo operacional**, clique no botão **Configurações**.

   A janela **Modo operacional** é exibida.
4. Execute as seguintes ações na janela **Modo operacional**:

   - Se desejar ativar o modo em que os recursos são concedidos a outros aplicativos, marque a caixa de seleção **Conceder recursos a outros aplicativos**.

     Com a configuração de conceder recursos a outros aplicativos, o Kaspersky Endpoint Security adia as tarefas agendadas que tornam os aplicativos mais lentos:

     - Tarefa de Atualização
     - Tarefa de Verificação Completa
     - Tarefa de Verificação de Áreas Críticas
     - Tarefa de Verificação Personalizada
     - Tarefa de Verificação de Vulnerabilidades
     - Tarefa de Verificação da Integridade
   - Se desejar desativar o modo em que os recursos são concedidos a outros aplicativos, desmarque a caixa de seleção **Conceder recursos a outros aplicativos**. Nesse caso, o Kaspersky Endpoint Security executa as tarefas agendadas seja qual for o modo de operação dos outros aplicativos.

   Por padrão, o aplicativo está configurado para conceder recursos a outros aplicativos.
5. Para salvar as alterações, clique no botão **Salvar**.

Proteção por senha

Esta seção contém informações sobre a restrição de acesso por senha ao Kaspersky Endpoint Security.

Sobre a restrição de acesso ao Kaspersky Endpoint Security

Vários usuários com diferentes níveis de conhecimentos de informática podem utilizar um computador. Se os usuários têm acesso sem restrições ao Kaspersky Endpoint Security e às configurações deste, talvez haja uma redução do nível geral de proteção.

É possível restringir o acesso ao Kaspersky Internet Security estipulando um nome de usuário e uma senha e especificando as operações nas quais o aplicativo solicita ao usuário suas credenciais:

Quando uma versão anterior do aplicativo é atualizada para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, a senha é preservada (se tiver sido definida). Para editar as configurações de proteção por senha pela primeira vez, utilize o nome de usuário padrão KLAdmin.

Ativar e desativar a proteção por senha

É recomendável ter os cuidados necessários ao usar uma senha para restringir o acesso ao aplicativo. Se você esquecer a senha, entre em contato com o Suporte Técnico da Kaspersky para obter instruções sobre como desativar a proteção da senha.

Para ativar a proteção por senha:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.

   As configurações do aplicativo são exibidas na parte direita da janela.
3. Na seção **Proteção por senha**, clique no botão **Configurações**.

   A janela **Proteção por senha** é exibida.
4. Marque a caixa de seleção **Ativar a proteção por senha**.
5. No campo **Nome de usuário**, insira o nome de usuário que deve ser especificado na janela **Verificação de senha** quando as operações subsequentes protegidas por senha forem executadas.
6. No campo **Nova senha**, digite uma nova senha de acesso ao aplicativo.
7. Confirme a senha no campo **Confirmar senha**.
8. Se desejar restringir o acesso de todas as operações com o aplicativo, na seção **Escopo da senha**, clique no botão **Selec. tudo**.
9. Se desejar restringir seletivamente o acesso do usuário, na seção **Escopo da senha**, selecione as caixas ao lado dos nomes das operações relevantes:
   - **Configurar configurações do aplicativo**.
   - **Sair do aplicativo**.
   - **Desativar componentes de proteção**.
   - **Desativar componentes de controle**.
   - **Remover a chave**.
   - **Remover / modificar / restaurar o aplicativo**.
   - **Restaurar acesso a dados em discos criptografados**.
   - **Visualize relatórios**.

10. Clique no botão **OK**.

    O aplicativo verifica as senhas inseridas. Se as senhas coincidirem, o aplicativo aplicará a senha. Se as senhas não coincidirem, o aplicativo solicitará que você confirme a senha novamente no campo **Confirmar senha**.

Depois que a proteção por senha for ativada, o aplicativo solicitará uma senha cada vez que uma operação incluída no escopo da senha for executada. Se não quiser que o aplicativo solicite a senha sempre que você tentar executar uma operação protegida por senha durante a sessão atual, marque a caixa de seleção **Salvar a senha da sessão atual** na janela **Verificação de senha**.

Quando a caixa de seleção **Salvar a senha da sessão atual** está desmarcada, o aplicativo solicita a senha cada vez que você tentar executar uma operação protegida por senha.

Para desativar a proteção de senha:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.

   As configurações do aplicativo são exibidas na parte direita da janela.
3. Na seção **Proteção por senha**, clique no botão **Configurações**.

   A janela **Proteção por senha** é exibida.
4. Desmarque a caixa de seleção **Ativar a proteção por senha**.

   Você pode desativar a Proteção por senha somente se estiver feito o login como KLAdmin. Não é possível desativar a proteção por senha se você estiver usando qualquer outra conta de usuário ou uma senha temporária.
5. Clique no botão **OK**.

Depois que a proteção por senha for desativada, o acesso restringido ao aplicativo será cancelado no momento da inicialização posterior do Kaspersky Endpoint Security.

Modificar a senha de acesso do Kaspersky Endpoint Security

Para alterar a senha de acesso do Kaspersky Endpoint Security:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.
3. Na seção **Proteção por senha**, clique no botão **Configurações**.

   A janela **Proteção por senha** é exibida.
4. Insira o nome de usuário no campo **Nome de usuário**.
5. No campo **Nova senha**, insira uma nova senha de acesso ao aplicativo.
6. No campo **Confirmar senha**, insira a nova senha novamente.
7. Clique em **OK**.

O aplicativo verifica as senhas inseridas. Se as senhas corresponderem, o aplicativo aplica a nova senha e fecha a janela **Proteção por senha**. Se as senhas não coincidirem, o aplicativo solicitará que você confirme a senha novamente no campo **Confirmar senha**.

8. Para salvar as alterações, na janela de configurações do aplicativo, clique no botão **Salvar**.

Sobre a utilização de uma senha temporária

Quando trabalhar em computadores de cliente gerenciados por uma política do Kaspersky Security Center, os usuários precisam executar operações com Kaspersky Endpoint Security que são protegidas por senha no nível de política. Quando a proteção por senha é ativada, só o administrador do Kaspersky Security Center pode executar as operações especificadas no escopo da senha. Contudo, se a conexão com Kaspersky Security Center foi perdida (tal como quando o usuário está fora da rede corporativa), funções para trabalhar com a interface local do Kaspersky Security Center são limitadas.

Para prover um usuário da capacidade de executar operações necessárias sem dar ao usuário a senha que é estabelecida nas configurações de política, o administrador do Kaspersky Security Center pode criar uma senha temporária. Uma senha temporária tem um período de validade limitado e um escopo de ação limitado. Depois que o usuário insere a senha temporária na interface local do aplicativo, as operações permitidas pelo administrador do Kaspersky Security Center ficam disponíveis.

Quando a senha temporária expira, o Kaspersky Endpoint Security continua funcionando conforme as configurações da política do Kaspersky Security Center. As operações que são protegidas por senha ao nível de política ficam indisponíveis ao usuário.

Criar uma senha temporária usando o Console de Administração do Kaspersky Security Center

Para criar uma senha temporária e enviá-la a um usuário:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos Gerenciados** da árvore de Console de Administração, abra a pasta com o nome do grupo de administração que inclui o computador do usuário que solicita a senha temporária.

3. No espaço de trabalho, selecione a guia **Dispositivos**.

4. No menu de contexto do computador que pertence ao usuário que solicita a senha temporária, selecione **Propriedades**.

   A janela **Propriedades: <Nome do computador>** é exibida.

5. Na janela **Propriedades: <Nome do computador>**, selecione a seção **Aplicativos**.

6. Selecione Kaspersky Endpoint Security Service Pack 2 for Windows e abra a janela de propriedades do aplicativo usando um dos seguintes métodos:

   - Clique no botão **Propriedades** na parte inferior da tela.

   - No menu de contexto do aplicativo, selecione **Propriedades**.

   Isto abre a janela **Configuração do aplicativo "<Nome do aplicativo>"**.

7. Na janela **Configuração do aplicativo "<Nome de aplicativo>"**, na seção **Configurações avançadas**, selecione a subseção **Configurações do aplicativo**.

8. Na seção **Proteção por senha**, clique no botão **Configurações**.

   A janela **Proteção por senha** é exibida.

9. Na janela **Proteção por senha**, na seção **Senha temporária**, clique no botão **Configurações**.

   > Este botão estará disponível se a Proteção por senha estiver ativada para o Kaspersky Security Center na política do Kaspersky Security Center que está sendo executado no computador.

   A janela **Criar senha temporária** é exibida.

10. No campo **Data de expiração**, especifique a data na qual o usuário não será mais capaz de usar a senha temporária.

    Nesta data, a senha temporária ficará inválida. Uma nova senha temporária deverá ser criada para permitir o acesso para executar operações na interface local do Kaspersky Endpoint Security.

11. Na tabela **Escopo da senha temporária**, marque as caixas de seleção ao lado das operações que devem estar disponíveis para o usuário enquanto a senha temporária é válida.

12. Clique no botão **Criar**.

    Isto abre a janela **Senha temporária** que contém uma senha criptografada.

13. Copie a senha e as instruções sobre a aplicação dela e envie ao usuário.

Aplicar uma senha temporária na interface do Kaspersky Endpoint Security

> Estas instruções são destinadas para usuários de computadores de cliente com Kaspersky Endpoint Security instalado.

Para aplicar uma senha temporária:

1. Abra a janela de configurações do aplicativo.

2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.

   As configurações do aplicativo são exibidas na parte direita da janela.

3. Na seção **Proteção por senha**, clique no botão de **Senha Temporária**.

   A janela de **Senha temporária** é exibida.

4. Marque a caixa de seleção **Ativar senha temporária**.

5. No campo de entrada, especifique a senha que foi obtida do administrador do Kaspersky Security Center.

6. Clique em **OK** para salvar as alterações.

Depois que a senha temporária é aplicada, as operações especificadas pelo administrador do Kaspersky Security Center ficarão disponíveis. A janela **Senha temporária** exibe a data de expiração da senha temporária e as operações permitidas.

Administração remota do aplicativo através do Kaspersky Security Center

Esta seção descreve a administração do Kaspersky Endpoint Security no Kaspersky Security Center.

Sobre gerenciar o aplicativo através do Kaspersky Security Center

O Kaspersky Security Center permite que você, de forma remota, instale e desinstale, inicie e interrompa o Kaspersky Endpoint Security, defina as configurações do aplicativo, altere o conjunto de componentes do aplicativo disponível, adicione chaves e inicie tarefas de atualização e verificação.

Para obter informação adicional sobre gerenciamento do aplicativo via Kaspersky Security Center que não é fornecida neste documento, consulte o *Guia do Administrador do Kaspersky Security Center*.

O aplicativo pode ser gerenciado através do Kaspersky Security Center utilizando o plug-in de administração do Kaspersky Endpoint Security.

A versão do plug-in de administração pode diferenciar da versão do Kaspersky Endpoint Security instalado no computador de cliente. Se a versão instalada do plug-in de administração tiver menos funcionalidade do que a versão instalada do Kaspersky Endpoint Security, as configurações das funções ausentes não são reguladas pelo plug-in de administração. Essas configurações podem ser modificadas pelo usuário na interface local do Kaspersky Endpoint Security.

Considerações especiais ao trabalhar com versões diferentes de plug-ins de administração

Você pode usar um plug-in de administração para modificar os seguintes itens:

- Políticas
- Perfis de políticas
- Tarefas de grupo
- Tarefas locais
- Configurações locais do Kaspersky Endpoint Security

Você poderá gerenciar o Kaspersky Endpoint Security via Kaspersky Security Center só se você tiver um plug-in de administração cuja versão seja igual a ou posterior à versão especificada nas informações a respeito da compatibilidade do Kaspersky Endpoint Security com o plug-in de administração. Você poderá ver a versão necessária mínima do plug-in de administração no arquivo installer.ini incluído no kit de distribuição.

Se algum componente for aberto, o plug-in de administração verificará as suas informações de compatibilidade. Se a versão do plug-in de administração for igual ou posterior à versão especificada nas informações de compatibilidade, você pode modificar as configurações deste componente. Caso contrário, não será possível usar o plug-in de administração para alterar as configurações do componente selecionado. Recomenda-se fazer um upgrade do plug-in de administração.

Alterando configurações anteriormente definidas usando uma versão posterior do plug-in de administração

Você pode usar uma versão posterior do plug-in de administração para modificar todas as configurações anteriormente definidas e configurar novas configurações que não estiveram presentes na sua versão usada anteriormente do plug-in de administração.

Para novas configurações, uma versão posterior do plug-in de administração atribui os valores padrões quando uma política, o perfil de política ou a tarefa são salvos pela primeira vez.

Depois de você modificar as configurações de uma política, perfil de política ou tarefa de grupo usando uma versão posterior do plug-in de administração, estes componentes ficarão indisponíveis para versões anteriores do plug-in de administração. As configurações locais do Kaspersky Endpoint Security e as configurações de tarefas locais ainda estão disponíveis para o plug-in de administração de versões anteriores.

Iniciar e interromper o Kaspersky Endpoint Security em um computador cliente

Para iniciar ou encerrar o aplicativo em um computador cliente:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertence o computador cliente desejado.
3. No espaço de trabalho, selecione a guia **Dispositivos**.
4. Selecione o computador em que deseja iniciar ou encerrar o aplicativo.
5. Clique com o botão direito para exibir o menu de contexto do computador cliente e selecione **Propriedades**.

   A janela de propriedades do computador cliente abre.
6. Na janela de propriedades do computador cliente, selecione a seção **Aplicativos**.

   A lista de aplicativos da Kaspersky que estão instalados no computador cliente aparece à direita da janela de propriedades do computador cliente.
7. Selecione o Kaspersky Endpoint Security 10 for Windows.
8. Faça o seguinte:

   - Para iniciar o aplicativo, clique no botão à direita da lista de aplicativos da Kaspersky ou faça o seguinte:

     a. Selecione **Propriedades** no menu de contexto do Kaspersky Endpoint Security ou clique no botão **Propriedades** localizado abaixo da lista de aplicativos da Kaspersky.

     A janela **Configurações dos aplicativos do Kaspersky Endpoint Security 10 for Windows** é aberta.

     b. Na seção **Geral**, clique no botão **Executar** na parte direita da janela.

   - Para encerrar o aplicativo, clique no botão à direita da lista de aplicativos da Kaspersky ou faça o seguinte:

     a. Selecione **Propriedades** no menu de contexto do Kaspersky Endpoint Security ou clique no botão **Propriedades** localizado abaixo da lista de aplicativos da Kaspersky.

     A janela **Configurações dos aplicativos do Kaspersky Endpoint Security 10 for Windows** é aberta.

b. Na seção **Geral**, clique no botão **Interromper** na parte direita da janela.

Definir as configurações do Kaspersky Endpoint Security

Para definir as configurações do Kaspersky Endpoint Security :

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertence o computador cliente desejado.
3. No espaço de trabalho, selecione a guia **Dispositivos**.
4. Selecione o computador no qual deseja definir as configurações do Kaspersky Endpoint Security.
5. No menu de contexto do computador cliente, selecione **Propriedades**.

   A janela de propriedades do computador cliente abre.
6. Na janela de propriedades do computador cliente, selecione a seção **Aplicativos**.

   A lista de aplicativos da Kaspersky que estão instalados no computador cliente aparece à direita da janela de propriedades do computador cliente.
7. Selecione o aplicativo Kaspersky Endpoint Security 10 for Windows.
8. Execute uma das seguintes ações:

   - Selecione **Propriedades** no menu de contexto do Kaspersky Endpoint Security 10 for Windows.
   - Clique no botão **Propriedades** abaixo da lista de aplicativos do Kaspersky.

   A janela **Configurações dos aplicativos do Kaspersky Endpoint Security 10 for Windows** é aberta.
9. Na seção **Configurações avançadas**, configure as configurações do Kaspersky Endpoint Security bem como as configurações de armazenamento e relatório.

   As outras seções da janela do **Configurações do aplicativo do Kaspersky Endpoint Security 10 for Windows** são as mesmas que as seções do aplicativo padrão do Kaspersky Security Center. Uma descrição dessas seções é fornecida no *Guia do Administrador do Kaspersky Security Center*.

   > Se um aplicativo estiver sujeito a uma política que proíbe modificações de configurações específicas, você não será capaz de editá-los definindo a configuração do aplicativo na seção **Configurações avançadas**.
10. Para salvar as suas alterações, na janela **Configurações do aplicativo Kaspersky Endpoint Security 10 for Windows**, clique em **OK**.

Gerenciar tarefas

Esta seção descreve como gerenciar as tarefas do Kaspersky Endpoint Security. Exiba o *Guia de Administrador do Kaspersky Security Center* para obter detalhes sobre o gerenciamento das tarefas através do Kaspersky Security Center.

Sobre as tarefas do Kaspersky Endpoint Security

O Kaspersky Security Center controla a atividade de aplicativos da Kaspersky nos computadores clientes usando tarefas. As tarefas implementam as principais funções de administração, como chave de instalação, verificação do computador e atualização dos bancos de dados e módulos do software aplicativo.

Você pode criar os seguintes tipos de tarefas na administração do Kaspersky Endpoint Security por meio do Kaspersky Security Center:

- Tarefas locais configuradas para um computador cliente individual.
- Tarefas de grupo configuradas para computadores clientes que pertencem aos grupos de administração
- Tarefas do grupo de computadores que não pertencem a grupos de administração.

  Tarefas para conjuntos de computadores que não pertencem aos grupos de administração aplicam-se somente aos computadores clientes especificados nas configurações da tarefa. Se novos computadores clientes forem adicionados a um conjunto de computadores para os quais uma tarefa é configurada, esta tarefa não se aplica a estes novos computadores. Para aplicar a tarefa a estes novos computadores, crie uma nova tarefa ou edite as configurações da tarefa existente.

Para gerenciar remotamente o Kaspersky Endpoint Security, você pode usar as seguintes tarefas de algum dos tipos listados:

- **Adicionar chave**. O Kaspersky Endpoint Security adiciona uma chave para ativação do aplicativo, incluindo uma chave adicional.
- **Alterar componentes do aplicativo**. O Kaspersky Endpoint Security instala ou remove componentes em computadores de cliente segundo a lista de componentes especificados nas configurações da tarefa.
- **Inventário**. O Kaspersky Endpoint Security coleta informações sobre todos os aplicativos executáveis que estão armazenados nos computadores.

  Você pode ativar o inventário de módulos DLL e arquivos de script. Nesse caso, o Kaspersky Security Center receberá informações sobre módulos DLL carregados em um computador com Kaspersky Endpoint Security instalado, e sobre arquivos que contêm scripts.

  Ativar o inventário de módulos DLL e arquivos de script aumenta de forma significativa a duração de tarefa de inventário e o tamanho de banco de dados.
- **Atualização**. O Kaspersky Endpoint Security atualiza bancos de dados e módulos do aplicativo segundo as configurações de atualização configuradas.
- **Reversão**. O Kaspersky Endpoint Security reverte a última atualização de bancos de dados e módulos.
- **Verificação de vírus**. O Kaspersky Endpoint Security verifica as áreas do computador especificadas nas configurações da tarefa para detectar vírus e outras ameaças.
- **Verificando conexão com KSN**. O Kaspersky Endpoint Security envia uma consulta sobre a disponibilidade de servidores KSN e atualiza o status de conexão de KSN.

- **Verificação da integridade**. O Kaspersky Endpoint Security recebe dados sobre o conjunto de módulos do aplicativo instalados no computador de cliente e verifica a assinatura digital de cada módulo.
- **Gerenciar contas do Agente de Autenticação**. Enquanto executa esta tarefa, o Kaspersky Endpoint Security gera comandos de remoção, adição ou modificação das contas do Agente de Autenticação.

Você pode executar as seguintes operações com as tarefas:

- Iniciar, interromper, suspender e reiniciar tarefas.
- Criar novas tarefas.
- Editar as configurações da tarefa.

Os direitos de acesso às configurações de tarefas do Kaspersky Endpoint Security (ler, gravar, executar) são definidos para cada usuário com acesso ao Servidor de Administração do Kaspersky Security Center através das configurações do acesso a áreas funcionais do Kaspersky Endpoint Security. Para configurar o acesso a áreas funcionais do Kaspersky Endpoint Security, acesse a seção **Segurança** da janela de propriedades do Servidor de Administração do Kaspersky Security Center.

Configurar o modo de gerenciamento das tarefas

Para configurar o modo para trabalhar com tarefas na interface local do Kaspersky Endpoint Security:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual você deseja configurar o modo para trabalhar com tarefas na interface local do Kaspersky Endpoint Security.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na seção **Configurações avançadas**, selecione a subseção **Configurações do aplicativo**.
7. Na seção **Modo operacional**:
   - Se desejar permitir que usuários trabalhem com tarefas locais na interface e na linha de comando do Kaspersky Endpoint Security, marque a caixa de seleção **Permitir uso de tarefas locais**.

     Se a caixa de seleção for desmarcada, as funções de tarefas locais serão interrompidas. Neste modo, as tarefas locais não são executadas de acordo com o agendamento. As tarefas locais também estão indisponíveis para iniciar e editar na interface local do Kaspersky Endpoint Security, e quando trabalhar com a linha de comando.

- Se desejar permitir que os usuários exibam a lista de tarefas de grupo, marque a caixa de seleção **Permitir que as tarefas do grupo sejam exibidas**.
- Se desejar permitir que usuários modifiquem as configurações de tarefas de grupo, marque a caixa de seleção **Permitir gerenciamento de tarefas do grupo**.

8. Clique em **OK** para salvar as alterações.
9. Aplique a política.

   Consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes sobre a aplicação da política do Kaspersky Security Center

Criar uma tarefa local

Para criar uma tarefa local:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertence o computador cliente desejado.
3. No espaço de trabalho, selecione a guia **Dispositivos**.
4. Selecione o computador para o qual você deseja criar uma tarefa local.
5. Execute uma das seguintes ações:
   - No menu de contexto do computador cliente, selecione a opção **Todas as tarefas** Criar tarefa.
   - No menu de contexto do computador cliente, selecione **Propriedades**, e na janela **Propriedades: <Nome do computador>** exibida, na guia **Tarefas**, clique no botão **Adicionar**.
   - Na lista suspensa **Executar ação**, selecione **Criar tarefa**.

   O Assistente de Tarefas é iniciado.
6. Siga as instruções do Assistente de Tarefas.

Criar uma tarefa de grupo

Para criar uma tarefa de grupo:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Execute uma das seguintes ações:
   - Selecione a pasta **Dispositivos gerenciados** na árvore do Console de Administração para criar uma tarefa de grupo para todos os computadores gerenciados pelo Kaspersky Security Center.
   - Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, selecione a pasta com o nome do grupo de administração ao qual pertence o computador cliente desejado.

3. Selecione a guia **Tarefas** no espaço de trabalho.
4. Clique no botão **Criar tarefa**.

   O Assistente de Tarefas é iniciado.
5. Siga as instruções do Assistente de Tarefas.

Criar uma tarefa para uma seleção de dispositivos

Para criar uma tarefa para seleção de dispositivo, execute o seguinte:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Selecione a pasta **Tarefas** na árvore do Console de Administração.
3. Clique no botão **Criar tarefa**.

   O Assistente de Tarefas é iniciado.
4. Siga as instruções do Assistente de Tarefas.
5. Na janela **Selecionar dispositivos aos quais a tarefa será atribuída** do Assistente, clique no botão **Atribuir tarefa a uma seleção de dispositivos**.
6. Na janela próxima ao Assistente, clique no botão **Selecionar**.

   A janela **Seleção de dispositivo** é exibida.
7. Selecione os dispositivos necessários.
8. Clique em **OK** na janela **Seleção do dispositivo**.
9. Siga as instruções do Assistente de Tarefas.

Iniciar, interromper, suspender e reiniciar uma tarefa

Se o aplicativo em execução do Kaspersky Endpoint Security estiver em um computador cliente, você pode iniciar, interromper, suspender e reiniciar uma tarefa nesse computador cliente por meio do Kaspersky Security Center. Quando o Kaspersky Endpoint Security está suspenso, as tarefas em execução são suspensas e não será possível iniciar, interromper, suspender ou reiniciar uma tarefa através do Kaspersky Security Center.

Para iniciar, interromper, suspender ou reiniciar uma tarefa local:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertence o computador cliente desejado.
3. No espaço de trabalho, selecione a guia **Dispositivos**.

4. Selecione o computador em que deseja iniciar, interromper, pausar ou reiniciar uma tarefa local.

5. Clique com o botão direito para exibir o menu de contexto do computador cliente e selecione **Propriedades**.

   A janela de propriedades do computador cliente abre.

6. Selecione a seção de **Tarefas**.

   A janela de tarefas aparece na parte direita da janela.

7. Selecione a tarefa local que deseja iniciar, encerrar, suspender ou continuar.

8. Execute a ação necessária na tarefa usando um dos seguintes métodos:

   - Clique com o botão direito para abrir o menu de contexto da tarefa local e selecione **Executar** / **Interromper** / **Pausar** / **Reiniciar**.
   - Para iniciar ou encerrar uma tarefa local, clique no botão / à direita da lista de tarefas locais.
   - Faça o seguinte:

     a. Clique no botão **Propriedades** abaixo da lista de tarefas local ou selecione **Propriedades** no menu de contexto da tarefa.

        A janela **Propriedades: <Nome da tarefa>** é exibida.

     b. Na guia **Geral**, clique no botão **Executar** / **Interromper** / **Pausar** / **Reiniciar**.

Para iniciar, encerrar, pausar ou continuar uma tarefa de grupo:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração em que deseja iniciar, interromper, pausar ou reiniciar a tarefa local.

3. Selecione a guia **Tarefas** no espaço de trabalho.

   As tarefas de grupo são exibidas na parte direita da janela.

4. Selecione uma tarefa de grupo que deseja iniciar, interromper, pausar ou reiniciar.

5. Execute a ação necessária na tarefa usando um dos seguintes métodos:

   - No menu de contexto da tarefa de grupo, selecione **Executar** / **Interromper** / **Pausar** / **Reiniciar**.
   - Clique no botão / à direta da janela para iniciar ou interromper uma tarefa de grupo.
   - Faça o seguinte:

     a. Clique no link **Configurações da Tarefa** na parte direita da área de trabalho de Console de administração ou selecione **Propriedades** no menu de contexto da tarefa.

        A janela **Propriedades: <Nome da tarefa>** é exibida.

     b. Na guia **Geral**, clique no botão **Executar** / **Interromper** / **Pausar** / **Reiniciar**.

Para iniciar, interromper, pausar ou reiniciar uma tarefa para uma seleção de computadores:

1. Abra o Console de Administração do Kaspersky Security Center.

2. Na pasta **Tarefas** na árvore do Console de Administração, selecione uma tarefa para uma seleção de computadores que deseja iniciar, interromper, pausar ou reiniciar.

3. Execute uma das seguintes ações:

   - No menu de contexto da tarefa, selecione **Executar** / **Interromper** / **Pausar** / **Reiniciar**.
   - Clique no botão / , na parte direita da janela, para iniciar ou interromper a tarefa de computadores específicos.
   - Faça o seguinte:

     a. Clique no link **Configurações da Tarefa** na parte direita da área de trabalho de Console de administração ou selecione **Propriedades** no menu de contexto da tarefa.

     A janela **Propriedades: <Nome da tarefa>** é exibida.

     b. Na guia **Geral**, clique no botão **Executar** / **Interromper** / **Pausar** / **Reiniciar**.

Editar as configurações da tarefa

Para editar as configurações de uma tarefa local:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertence o computador cliente desejado.
3. No espaço de trabalho, selecione a guia **Dispositivos**.
4. Selecione um computador para o qual você deseja definir a configuração do aplicativo.
5. Clique com o botão direito para exibir o menu de contexto do computador cliente e selecione **Propriedades**.

   A janela de propriedades do computador cliente abre.
6. Selecione a seção de **Tarefas**.

   A janela de tarefas aparece na parte direita da janela.
7. Selecione a tarefa local desejada na lista de tarefas locais.
8. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
9. Na janela **Propriedades:<Nome da tarefa de grupo>**, selecione a seção **Configurações**.
10. Edite as configurações da tarefa local.
11. Para salvar as alterações, na janela **Propriedades: <Nome da tarefa local>** clique em **OK**.
12. Para salvar as alterações, na janela **Propriedades: <Nome do computador>**, clique em **OK**.

Para editar as configurações de uma tarefa de grupo:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados**, abra a pasta com o nome do grupo de administração desejado.
3. Selecione a guia **Tarefas** no espaço de trabalho.
   As tarefas de grupo são exibidas na área de trabalho de Console de administração.
4. Selecione a tarefa de grupo necessária.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
6. Na janela **Propriedades: <Nome da tarefa de grupo>**, selecione a seção **Configurações**.
7. Edite as configurações da tarefa de grupo.
8. Para salvar as alterações, na janela **Propriedades: <Nome da tarefa do grupo>** clique em **OK**.

Para editar as configurações de uma tarefa para um conjunto de computadores:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Tarefas** na árvore do Console de Administração, selecione uma tarefa para um conjunto de computadores cujas configurações deseja editar.
3. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.
4. Na janela **Propriedades: <Nome de uma tarefa para um conjunto de computadores>**, selecione a seção **Configurações**.
5. Edite as configurações da tarefa da seleção de computadores.
6. Para salvar as alterações, na janela **Propriedades: <Nome da tarefa para uma seleção de computadores>** clique em **OK**.

Exceto a seção **Configurações**, todas as seções na janela de propriedades da tarefa são idênticas àquelas usadas no Kaspersky Security Center. Para obter informações detalhadas, consulte o Guia do Administrador do *Kaspersky Security Center*. A seção **Configurações** contém as configurações específicas para o Kaspersky Endpoint Security 10 for Windows. Seu conteúdo depende da tarefa selecionada ou do tipo de tarefa.

Gerenciamento de políticas

Esta seção trata da criação e configuração de políticas para o Kaspersky Endpoint Security. Para obter informação mais detalhada sobre como gerenciar o Kaspersky Endpoint Security usando políticas do Kaspersky Security Center, consulte o *Guia de Administrador de Kaspersky Security Center*.

Sobre as políticas

Estabelecer políticas permite que você aplique configurações de aplicativo universais para todos os computadores clientes em um grupo de administração.

Você pode alterar localmente os valores das configurações especificadas por uma política para computadores individuais em um grupo de administração utilizando o Kaspersky Endpoint Security. Você pode alterar localmente apenas as configurações cuja modificação não é proibida pela política.

A possibilidade de a configuração do aplicativo em um computador cliente ser editada é determinada pelo status "bloqueio" da configuração no âmbito da política:

- Se uma definição for bloqueada (), você não pode editar localmente o valor dessa definição. O valor da configuração especificado pela política é utilizado para todos os computadores dos clientes no grupo de administração.

- Quando a configuração está desbloqueada (), é possível editá-la localmente. A definição configurada localmente é aplicada a todos os computadores clientes no âmbito do grupo de administração. A configuração de políticas não é aplicada.

Após a política ser aplicada pela primeira vez, as configurações locais do aplicativo mudam de acordo com as configurações da política.

Os direitos de acesso às configurações da política (ler, gravar, executar) são especificados para cada usuário com acesso ao Servidor de Administração do Kaspersky Security Center e separadamente para cada escopo funcional do Kaspersky Endpoint Security. Para configurar os direitos de acesso a configurações da política, acesse a seção **Segurança** da janela de propriedades do Servidor de Administração do Kaspersky Security Center.

Os escopos funcionais seguintes do Kaspersky Endpoint Security são separados:

- Proteção antivírus. O escopo funcional inclui o Antivírus de Arquivos, Antivírus de E-mail, Antivírus da Web, Antivírus de MI, Verificação de Vulnerabilidades e tarefas de verificação.

- Controle de Inicialização de Aplicativo. O escopo funcional inclui o componente Controle de inicialização de aplicativo.

- Controle de Dispositivo. O escopo funcional inclui o componente Controle de Dispositivo.

- Criptografia. O escopo funcional inclui os componentes de criptografia de discos rígidos, arquivos e pastas.

- Zona confiável. O escopo funcional inclui a Zona Confiável.

- Controle da Web. O escopo funcional inclui o componente Controle da Web.

- Prevenção de invasões. Este escopo funcional inclui o Monitoramento de Atividades do Aplicativo, o Monitoramento de Vulnerabilidades, o Firewall, o Bloqueador de Ataques a Rede e o Controle de Privilégios de Aplicativo.

- Funcionalidade básica. Esse escopo funcional inclui as configurações gerais do aplicativo que não são especificadas para outros escopos funcionais, incluindo: licenças, configurações do KSN, tarefas de inventário, tarefas de atualização de bancos de dados e de módulos do aplicativo, Autodefesa, configurações avançadas do aplicativo, relatórios e armazenamentos, configurações da proteção por senha e configurações da interface do aplicativo.

Você pode executar as seguintes operações com a política:

- Criar uma política.
- Editar as configurações da política.

  Se a conta do usuário com a qual você acessou o Servidor de Administração não tiver direitos para editar configurações de alguns escopos funcionais, as configurações desses escopos funcionais não estão disponíveis para edição.

- Excluir política.
- Alterar o status da política.

Para obter informações sobre a utilização de políticas que não são relacionadas à interação com o Kaspersky Endpoint Security, consulte o *Guia de Administrador do Kaspersky Security Center*.

Criar uma política

Para criar uma política:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Execute uma das seguintes ações:
   - Selecione a pasta **Dispositivos gerenciados** na árvore do Console de Administração para criar uma política para todos os computadores gerenciados pelo Kaspersky Security Center.
   - Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, selecione a pasta com o nome do grupo de administração ao qual pertence o computador cliente desejado.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Execute uma das seguintes ações:
   - Clique no botão **Criar política**.
   - Clique com o botão direito do mouse para abrir o menu de contexto e selecione **Criar** Política.

   O Assistente de Políticas é iniciado.
5. Siga as instruções do Assistente de Políticas.

Editar as configurações da política

Para editar as configurações da política:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** na árvore do Console de Administração, abra a pasta com o nome do grupo de administração para o qual deseja editar as configurações da política.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Selecione a política desejada.
5. Abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique no link **Configurar política**, localizado na parte direita da área de trabalho do Console de Administração.

   As configurações de política do Kaspersky Endpoint Security 10 for Windows incluem as configurações de componentes e as configurações do aplicativo. As seções **Proteção antivírus** e **Controle de Endpoints** da janela **Propriedades: <Nome de política>** exibem as configurações da proteção e componentes de controle, a seção **Criptografia de dados** exibe as configurações de criptografia para arquivos e pastas, e a seção de **Configurações avançadas** exibe as configurações do aplicativo.

   Para ativar a exposição das configurações de criptografia de dados e configurações de componentes de controle nas configurações da política, você deve marcar as caixas de seleção correspondentes na janela **de Configurações de Interface** do Kaspersky Security Center.
6. Editar as configurações da política.
7. Para salvar as alterações, na janela **Propriedades: <Nome de política>**, clique em **OK**.

Selecionar configurações a serem exibidas na política do Kaspersky Security Center

Para selecionar as configurações a serem exibidas na política do Kaspersky Security Center:

1. Abra o Console de Administração do Kaspersky Security Center.
2. No menu de contexto do nó **Servidor de Administração – <Nome do computador>** da árvore do Console de Administração, selecione Exibir → **Configurações da interface**.

   A janela **Configurações da interface** é exibida.
3. Na janela **Configurações de Interface**, marque as caixas de seleção ao lado das configurações que devem ser exibidas nas configurações de criação de política do Kaspersky Security Center e nas propriedades de política:
   - Marque a caixa de seleção **Exibir componentes de controle de endpoints** para ativar a exibição das configurações do componente de controle na janela do Novo Assistente de Políticas do Kaspersky Security Center e nas propriedades da política.
   - Marque a caixa de seleção **Exibir criptografia e proteção de dados** para ativar a exibição das configurações de criptografia de dados na janela do Novo Assistente de Políticas do Kaspersky Security Center e nas propriedades da política.

4. Clique em **OK**.

Enviar mensagens de usuário ao servidor do Kaspersky Security Center

Talvez um usuário precise enviar uma mensagem ao administrador de rede corporativa local nos seguintes casos:

- Acesso bloqueado do Controle de Dispositivo ao dispositivo.

  O modelo da mensagem de uma solicitação para acessar um dispositivo bloqueado está disponível na interface Kaspersky Endpoint Security na seção Controle de Dispositivo.

- O Controle de Inicialização de Aplicativo bloqueou a inicialização de um aplicativo.

  O modelo de mensagem de uma solicitação de permitir a inicialização de um aplicativo bloqueado está disponível na interface do Kaspersky Endpoint Security na seção Controle de Inicialização de Aplicativo.

- Acesso bloqueado do Controle da Web ao recurso da Web.

  O modelo de mensagem de uma solicitação para acessar um recurso da Web bloqueado está disponível na interface do Kaspersky Endpoint Security na seção Controle da Web.

O método usado para enviar mensagens e o modelo utilizado depende de haver ou não uma política do Kaspersky Security Center ativa em execução no computador que possui o Kaspersky Endpoint Security instalado e de haver ou não uma conexão com o servidor de administração do Kaspersky Security Center. Os seguintes cenários são possíveis:

- Se uma política do Kaspersky Security Center não estiver executando no computador que possui o Kaspersky Security Center instalado, a mensagem de um usuário será enviada ao administrador de rede local por e-mail.

  Os campos de mensagem são preenchidos com os valores de campos do modelo definido na interface local do Kaspersky Endpoint Security.

- Se uma política do Kaspersky Security Center estiver em execução no computador que possui o Kaspersky Security Center instalado, a mensagem padrão será enviada ao Servidor de administração do Kaspersky Security Center.

  Nesse caso, as mensagens de usuário estão disponíveis para exibição no Armazenamento de eventos do Kaspersky Security Center. Os campos de mensagem são povoados com os valores de campos do modelo definido na política do Kaspersky Security Center.

- Se uma política desatualizada do Kaspersky Security Center estiver em execução no computador com o Kaspersky Endpoint Security instalado, o método usado para enviar mensagens dependerá se há ou não uma conexão com Kaspersky Security Center.

  - Se uma conexão com o Kaspersky Security Center for estabelecida, o Kaspersky Endpoint Security enviará a mensagem padrão ao Servidor de administração do Kaspersky Security Center.

  - Se uma conexão com o Kaspersky Security Center estiver ausente, a mensagem de um usuário será enviada ao administrador de rede local por e-mail.

  Em ambos os casos, os campos de mensagem são preenchidos com os valores de campos do modelo definido na política do Kaspersky Security Center.

Visualizar as mensagens do usuário no armazenamento de eventos do Kaspersky Security Center

Os componentes Controle de Inicialização de Aplicativo, Controle de Dispositivo e Controle da Web ativam a usuários da rede local com computadores em que o Kaspersky Endpoint Security está instalado para enviar mensagens ao administrador.

Um usuário pode enviar mensagens ao administrador de duas formas:

- Como evento no armazenamento de eventos do Kaspersky Security Center.

  O evento do usuário é enviado ao armazenamento de eventos do Kaspersky Security Center se o aplicativo do Kaspersky Endpoint Security que está instalado no computador do usuário estiver sendo utilizado sob uma política ativa.

- Como mensagem de e-mail.

  As informações de usuário são enviadas pelo e-mail se o aplicativo do Kaspersky Endpoint Security instalado no computador do usuário não estiver executando sob uma política ou estiver executando sob uma política externa.

Para visualizar uma mensagem do usuário no armazenamento de eventos do Kaspersky Security Center:

1. Abra o Console de Administração do Kaspersky Security Center.
2. No nó **Servidor de administração** da árvore do Console de Administração, selecione a guia **Eventos**.

   A área de trabalho do Kaspersky Security Center exibe todos os eventos que ocorrem durante a operação do Kaspersky Endpoint Security, inclusive mensagens ao administrador que são recebidas de usuários da rede local.
3. Para configurar o filtro de evento, na lista suspensa **Seleção de eventos**, selecione **Solicitações de Usuário**.
4. Selecione a mensagem a enviar ao administrador.
5. Abra a janela **Configurações do evento** de uma das seguintes formas:

   - Clique no evento com o botão direito. No menu de contexto aberto, selecione **Propriedades**.
   - Clicar no botão **Abrir janela de propriedades de evento** na parte direita da área de trabalho do Console de administração.

Participar no Kaspersky Security Network

Esta seção contém informações sobre a participação no Kaspersky Security Network e as instruções para ativar e desativar o Kaspersky Security Network.

Sobre a participação no Kaspersky Security Network

Para melhorar a proteção do computador, o Kaspersky Endpoint Security usa dados que são coletados de usuários em todo o mundo. O *Kaspersky Security Network* foi projetado para coletar tais dados.

O Kaspersky Security Network (KSN) é uma infraestrutura de serviços em nuvem que permite o acesso à Base de Dados de Conhecimento on-line da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software. O uso dos dados do Kaspersky Security Network assegura rapidez nas respostas do Kaspersky Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos.

Dependendo da localização da sua infraestrutura, existe um serviço do KSN Global (a infraestrutura está alojada em servidores da Kaspersky) e um serviço KSN Particular (a infraestrutura é alojada por servidores terceiros; por exemplo, na rede do provedor de serviços da Internet).

Após alterar a licença, envie os detalhes da nova chave ao provedor de serviços para poder usar o KSN Particular. Caso contrário, a troca de dados com o KSN não será possível.

A participação dos usuários no KSN permite à Kaspersky coletar rapidamente as informações sobre tipos e fontes de ameaças, criar soluções para eliminá-las e reduzir o número de falsos alarmes exibidos pelos componentes do aplicativo.

Durante a participação no KSN, o aplicativo automaticamente envia estatísticas geradas durante o funcionamento do aplicativo para o KSN. O aplicativo também pode enviar à Kaspersky certos arquivos (ou partes de arquivos) que os criminosos podem usar para prejudicar o computador ou dados, para verificação adicional.

Nenhum dado pessoal do usuário é coletado, processado ou armazenado. Para obter informação mais detalhada sobre o envio à Kaspersky de informações estatísticas que são geradas durante a participação no KSN e sobre o armazenamento e a destruição de tais informações, consulte a Declaração do Kaspersky Security Network e o site da Kaspersky. O arquivo .ksn_<ID do idioma>.txt com o texto da Declaração do Kaspersky Security Network é incluído no kit de distribuição do aplicativo.

Para reduzir a carga nos servidores do KSN, a Kaspersky poderá lançar bancos de dados antivírus do aplicativo que podem desativar temporariamente ou limitar parcialmente os pedidos ao Kaspersky Security Network. Nesse caso, o status da conexão ao KSN aparece como *Ativado com restrições*.

Computadores de usuários gerenciados pelo Servidor de Administração do Kaspersky Security Center podem interagir com a KSN por meio do serviço de Proxy da KSN.

O serviço de Proxy da KSN fornece os seguintes recursos:

- O computador do usuário pode consultar o KSN e envia informações para o KSN, mesmo sem estar com acesso direito à Internet.
- O KSN Proxy armazena em cache os dados processados, dessa forma reduzindo a carga na conexão de rede externa e acelerando recebimento de informações solicitadas pelo computador do usuário.

Mais detalhes sobre o serviço Proxy do KSN podem ser encontrados no *Guia de Administrador do Kaspersky Security Center*.

As configurações do serviço Proxy do KSN podem ser definidas nas propriedades do *Kaspersky Security Center* política.

A participação no Kaspersky Security Network é opcional. O aplicativo convida o usuário a participar em KSN durante a configuração inicial do aplicativo. Os usuários podem iniciar ou descontinuar a participação no KSN a qualquer momento.

Ativar e desativar o Kaspersky Security Network

Para ativar o Kaspersky Security Network:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Configurações do KSN**.

   As configurações do Kaspersky Security Network são exibidas na parte direita da janela.
3. Execute uma das seguintes ações:
   - Se desejar ativar o uso do Kaspersky Security Network, selecione a caixa de seleção **Aceito a Declaração KSN e os termos de participação**.
   - Para desativar o uso do Kaspersky Security Network, desmarque a caixa de seleção **Aceito a Declaração KSN e os termos de participação**.
4. Para salvar as alterações, clique no botão **Salvar**.

Verificar a conexão ao Kaspersky Security Network

Para verificar a conexão ao Kaspersky Security Network:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no botão **Kaspersky Security Network**.

   A janela **Kaspersky Security Network** é exibida.

   A parte esquerda da janela **Kaspersky Security Network** mostra o modo da conexão ao Kaspersky Security Network na forma de um botão **KSN** redondo:
   - Se o Kaspersky Endpoint Security não estiver conectado ao Kaspersky Security Network, o botão **KSN** será exibido em cinza. O status que é exibido abaixo do botão **KSN** indica *Desativado*.

- Se o Kaspersky Endpoint Security estiver conectado ao Kaspersky Security Network e os servidores KSN estiverem disponíveis, o botão **KSN** será exibido em verde. As seguintes informações são exibidas sob o botão **KSN**: status *Ativado*, tipo de KSN em uso – **KSN Particular** ou **KSN Global** e a data e hora da última sincronização com os servidores KSN. A parte direita da janela exibe as estatísticas da reputação dos arquivos, recursos de Web e software.

O Kaspersky Endpoint Security coleta dados estatísticos relativos ao uso do KSN quando você abre a janela **Kaspersky Security Network**. As estatísticas não são atualizadas em tempo real.

- Se o Kaspersky Endpoint Security estiver conectado ao Kaspersky Security Network, mas os servidores KSN estiverem indisponíveis, o botão **KSN** é exibido em vermelho. O status que é exibido abaixo do botão **KSN** indica *Ativado*.

  Se a hora da última sincronização com os servidores do KSN exceder 15 minutos ou tiver o status *Desconhecido*, isso significa que os servidores do KSN estão indisponíveis. Em tal situação, você é recomendado a contatar o Suporte Técnico ou o seu provedor de serviços.

  A inexistência de conexão ao Kaspersky Security Network pode ser ocasionada pelos seguintes motivos:

  - O computador não está conectado à Internet.
  - O aplicativo não foi ativado ou a licença expirou.
  - Foram detectados problemas relacionados à chave foram (por exemplo, a chave foi colocada na lista negra).

Verificar a reputação de um arquivo np Kaspersky Security Network

O serviço KSN deixa que você recupere informações sobre aplicativos incluídos em bancos de dados de reputação do Kaspersky. Isto ativa o gerenciamento flexível de políticas de inicialização do aplicativo no nível de empresa, evitando assim a inicialização do adware e outros programas que podem ser usados por criminosos para danificar o seu computador ou dados pessoais.

Para verificar a reputação de um arquivo no Kaspersky Security Network:

1. Clique com o botão direito do mouse para ver o menu de contexto do arquivo cuja reputação você quer verificar.
2. Selecione a opção **Verificar reputação no KSN**.

Essa opção estarfá disponível se você tiver aceitado os termos da Declaração do Kaspersky Security Network.

Isso abre a janela **<Nome do arquivo> - Reputação no KSN**. A janela **<Nome do arquivo> - Reputação no KSN** exibe as seguintes informações sobre o arquivo que é verificado:

- **Caminho**. O caminho no qual o arquivo é salvo no disco.
- **Versão**. A versão do aplicativo (as informações são exibidas apenas para arquivos executáveis).

- **Assinatura digital**. Presença de uma assinatura digital com o arquivo.
- **Assinado**. A data na qual o certificado foi assinado com uma assinatura digital.
- **Criado**. Data de criação do arquivo.
- **Modificado**. Data da última modificação do arquivo.
- **Tamanho**. O espaço em disco ocupado pelo arquivo.
- Informações sobre quantos usuários confiam no arquivo ou bloqueiam o arquivo.

Proteção melhorada com o Kaspersky Security Network

A Kaspersky oferece um nível extra de proteção aos usuários através do Kaspersky Security Network. Esse método de proteção foi concebido para combater ameaças avançadas persistentes e ataques de dia zero. As tecnologias de nuvem integradas e o conhecimento dos analistas de vírus da Kaspersky tornam o Kaspersky Endpoint Security na escolha perfeita para obter proteção contra as mais sofisticadas ameaças de rede.

Os detalhes sobre proteção avançada do Kaspersky Endpoint Security estão disponíveis no site da Kaspersky.

Fontes de informação sobre o aplicativo

Página Kaspersky Endpoint Security no site da Kaspersky

Na página Kaspersky Endpoint Security você pode ver as informações gerais sobre o aplicativo, suas funções e recursos.

A página Kaspersky Endpoint Security contém um link para a loja virtual. Aqui você pode comprar ou renovar o aplicativo.

Página Kaspersky Endpoint Security na Base da Dados de Conhecimento

A *Base de Dados de Conhecimento* é uma seção no site de Suporte Técnico.

Na página Kaspersky Endpoint Security da Base de Dados de Conhecimento, você pode ler artigos sobre os recursos que fornecem informação útil, recomendações e respostas a perguntas frequentemente feitas sobre como comprar, instalar e usar o aplicativo.

Os artigos de Base de Conhecimento podem responder a perguntas que se relacionam não somente ao Kaspersky Endpoint Security mas também a outros aplicativos da Kaspersky. Os artigos na Base de Conhecimento também podem conter notícias do Suporte Técnico.

Discutir os aplicativos da Kaspersky no Fórum

Se a sua pergunta não precisar de uma resposta urgente, você poderá discuti-la com os especialistas da Kaspersky e com outros usuários no nosso Fórum.

Neste fórum, você pode visualizar os tópicos existentes, deixar seus comentários e criar tópicos de discussão novos.

Entrar em contato com o Suporte Técnico

Esta seção descreve como obter suporte técnico e os termos nos quais ele está disponível.

Como obter suporte técnico

Se você não puder encontrar uma solução para o seu problema na documentação do aplicativo ou em uma das fontes de informação sobre o aplicativo, recomendamos entrar em contato com o Suporte Técnico. Os especialistas do Suporte Técnico responderão às suas perguntas sobre instalação e uso do aplicativo.

O suporte técnico está disponível apenas para usuários que compraram uma licença comercial. Os usuários que receberam uma licença de teste não têm direito ao suporte técnico.

Antes de entrar em contato com o Suporte Técnico, leia as regras de suporte.

Você pode entrar em contato com o Suporte Técnico das seguintes formas:

- Chamando o Suporte Técnico por telefone
- Enviando uma solicitação ao Suporte Técnico do Kaspersky através do Portal Kaspersky CompanyAccount

Suporte técnico por telefone

Você pode ligar para os representantes do Suporte Técnico da maior parte das regiões em todo o mundo. Você pode encontrar informações sobre as formas de receber o suporte técnico na sua região e os contatos do Suporte Técnico no site do Suporte Técnico da Kaspersky.

Antes de entrar em contato com o Suporte Técnico, leia as regras de suporte.

Suporte técnico através do Kaspersky CompanyAccount

Kaspersky CompanyAccount é um portal para as empresas que utilizam aplicativos da Kaspersky. O portal Kaspersky CompanyAccount foi concebido para facilitar a interação entre os usuários e os especialistas da Kaspersky através de solicitações eletrônicas. Você pode usar o portal Kaspersky CompanyAccount para rastrear o status das suas solicitações eletrônicas e guardar um histórico dessas solicitações.

Você pode registrar todos os colaboradores da sua organização em uma única conta no Kaspersky CompanyAccount. Uma única conta permite que você gerencie de forma centralizada as solicitações eletrônicas dos colaboradores registrados na Kaspersky e também permite gerenciar os privilégios desses colaboradores 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.

Coletar Informações do Suporte Técnico

Após informar o problema encontrado aos especialistas do Suporte Técnico da Kaspersky, eles talvez solicitem que você crie um *arquivo de rastreamento*. O arquivo de rastreamento permite rastrear o processamento de comandos do aplicativo, etapa a etapa, e determinar em que estágio da operação do aplicativo o erro ocorreu.

Os especialistas do Suporte técnico podem solicitar informações adicionais sobre o sistema operacional, os processos sendo executados no computador, os relatórios detalhados sobre a operação de componentes do aplicativo e os despejos de memória do aplicativo.

Você poderá obter ajuda do Kaspersky Endpoint Security para coletar as informações necessárias. As informações coletadas podem ser salvas no disco rígido e carregadas posteriormente quando for mais conveniente para você.

Enquanto executa o diagnóstico, os especialistas do Suporte Técnico podem lhe pedir para alterar as configurações do aplicativo, da seguinte forma:

- A ativação da funcionalidade que coleta informações de diagnóstico adicionais.
- Otimizar as configurações de componentes individuais do aplicativo, as quais não estão disponíveis através de elementos da interface de usuário padrão.
- Alterar as configurações de armazenamento e transmissão de informações de diagnóstico que são coletadas.
- Configurar a intercepção e registro de tráfego de rede.

Os especialistas do Suporte Técnico irão fornecer todas as informações necessárias para executar essas operações (descrição da sequência de etapas, configurações a modificar, arquivos de configuração, scripts, funcionalidades adicionais da linha de comando, módulos de depuração, utilitários de finalidades especiais, etc.) e irão informá-lo sobre o escopo dos dados coletados para efeitos de depuração. As informações de diagnóstico adicionais coletadas são salvas no computador do usuário. Os dados coletados não são transmitidos automaticamente à Kaspersky.

As configurações utilizadas para determinar o endereço do servidor de dump para enviar arquivos de dump à Kaspersky são armazenadas no computador do usuário. Se necessário, os valores dessas configurações podem ser editados na chave de registro do sistema operacional `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"`.

As operações listadas em cima devem ser executadas sob a supervisão de especialistas do Suporte Técnico, seguindo suas instruções. As alterações não monitoradas a configurações do aplicativo, efetuadas de forma diferente do descrito no Guia do Administrador ou das instruções dos especialistas do Suporte Técnico podem abrandar ou bloquear o sistema operacional, afetar a segurança do computador ou comprometer a disponibilidade e integridade dos dados processados.

Criar um arquivo de rastreamento

Para criar o arquivo de rastreamento:

1. Abra a janela principal do aplicativo.
2. Na janela de aplicativo principal, clique no botão .

   A janela **Suporte** é exibida.
3. Na janela **Suporte**, clique no botão **Rastreamento de sistema**.

   A janela **Informações do Suporte Técnico** é aberta.
4. Para iniciar o processo de rastreamento, selecione a caixa de seleção **Ativar o rastreamento**.
5. Na lista suspensa **Nível**, selecione o nível de rastreamento.

   É recomendável obter mais informações sobre o nível de rastreamento junto de um especialista do Suporte Técnico. Caso não exista orientação do Suporte técnico, defina o nível de rastreamento para **Normal (500)**.
6. Reproduza a situação em que o problema ocorreu.
7. Para interromper o processo de rastreamento, volte à janela **Informações do Suporte Técnico** e desmarque a caixa de seleção **Ativar o rastreamento**.

Após criar o arquivo de rastreio, realize o carregamento dos resultados do rastreamento para o servidor da Kaspersky.

Conteúdo e armazenamento de arquivos de rastreio

O usuário é pessoalmente responsável por garantir a segurança dos dados coletados, especialmente pelo monitoramento e restrição de acesso aos dados coletados armazenados no computador até serem enviados para a Kaspersky.

Os arquivos de rastreio são armazenados no seu computador em formulário modificado que não pode ser lido desde que o aplicativo esteja sendo usado e são excluídos permanentemente quando o aplicativo é removido.

Os arquivos de rastreio são armazenados na pasta ProgramData\Kaspersky Lab.

O arquivo de rastreio possui o seguinte formato de nome: `KES<version number_dateXX.XX_timeXX.XX_pidXXX.><tipo de arquivo de rastreio>.log.enc1`.

O arquivo de rastreamento do Agente de Autenticação é armazenado na pasta de Informações sobre Volume do Sistema tem o seguinte nome: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Você pode visualizar os dados salvos em arquivos de rastreio. Entre em contato com o Suporte Técnico da Kaspersky para obter conselhos sobre como visualizar dados.

Todos os arquivos de rastreio contêm os seguintes dados comuns:

- Hora do evento.
- Número do thread de execução.

  O arquivo de rastreio do Agente de Autenticação não contém essas informações.

- Componente do aplicativo que causou o evento.
- Grau de gravidade do evento (evento informativo, aviso, evento crítico, erro).
- Uma descrição do evento envolvendo a execução de comando por parte de um componente do aplicativo e o resultado da execução desse comando.

Conteúdo dos arquivos de rastreio SRV.log, GUI.log e ALL.log

Os arquivos de rastreio SRV.log, GUI.log e ALL.log podem armazenar as seguintes informações, além dos dados gerais:

- Dados pessoais, incluindo o nome próprio, sobrenome e nome do meio, caso esses dados sejam incluídos no caminho de arquivos em um computador local.
- O nome de usuário e a senha, caso tenha sido transmitidos abertamente. Esses dados podem ser registrados em arquivos de rastreio durante a verificação de tráfego da Internet. O tráfego é registrado em arquivos de rastreio somente a partir de trafmon2.ppl.
- O nome de usuário e a senha, caso sejam incluídos em cabeçalhos HTTP.
- O nome da conta do Microsoft Windows, caso seja incluído em um nome de arquivo.
- O seu endereço de e-mail ou um endereço da Web com o nome da sua conta e senha, caso sejam ambos incluídos no nome do objeto detectado.
- Os sites que você visita e os redirecionamentos a partir desses sites. Esses dados são gravados em arquivos de rastreio quando o aplicativo verifica sites.
- O endereço do servidor proxy, nome do computador, porta, endereço IP e nome de usuário usado para fazer login no servidor proxy. Esses dados são registrados em arquivos de rastreio caso o aplicativo use um servidor proxy.
- Os endereços de IP remotos aos quais o computador estabeleceu conexões.
- Assunto da mensagem, ID, nome do remetente e endereço da página da Web do remetente da mensagem em uma rede social. Estes dados são escritos para rastrear os arquivos se o componente Controle da Web for ativado.

Conteúdo de arquivos de rastreio HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Além dos dados gerais, o arquivo de rastreio HST.log contém informações sobre a execução de uma tarefa de atualização do banco de dados e módulos do aplicativo.

Além de incluir dados gerais, o arquivo de rastreio BL.log contém informações sobre eventos que ocorrem durante a operação do aplicativo, bem como os dados requeridos para corrigir erros do aplicativo. Esse arquivo é criado se o aplicativo for iniciado com o parâmetro avp.exe –bl.

Além de incluir dados gerais, o arquivo de rastreio Dumpwriter.log contém informações de serviço requeridas para corrigir erros que ocorrem quando o arquivo de dump do aplicativo é gravado.

Além dos dados gerais, o arquivo de rastreio WD.log contém informações sobre eventos que ocorrem durante a operação do serviço avpsus, incluindo eventos de atualização do módulo do aplicativo.

Além dos dados gerais, o arquivo de rastreio AVPCon.dll.log contém informações sobre eventos que ocorrem durante a operação do módulo de conectividade do Kaspersky Security Center.

Conteúdo de arquivos de rastreio dos plug-ins do aplicativo

Os arquivos de rastreio dos plug-ins do aplicativo incluem as seguintes informações, além dos dados gerais:

- O arquivo de rastreio shellex.dll.log do plug-in que inicia a tarefa de verificação a partir do menu de contexto contém informações sobre a execução da tarefa de verificação e dados necessários para depurar o plug-in.
- O arquivo de rastreio mcou.OUTLOOK.EXE do plug-in de Antivírus de E-mail pode conter partes de mensagens de e-mail, incluindo endereços de e-mail.

Conteúdo do arquivo de rastreio do Agente de Autenticação

Além dos dados gerais, o arquivo de rastreio do Agente de Autenticação contém informações sobre a operação do Agente de Autenticação e as ações realizadas pelo usuário com o Agente de Autenticação.

Ativar ou desativar a transmissão de arquivos de dump e arquivos de rastreio para a Kaspersky

Para ativar ou desativar a transmissão de arquivos de rastreio e dump para a Kaspersky:

1. Abra a janela de configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Configurações Avançadas**.

   As configurações avançadas do aplicativo são exibidas na parte direita da janela.
3. Na seção **Modo operacional**, clique no botão **Configurações**.

   A janela **Modo operacional** é exibida.
4. Na janela **Modo operacional**, selecione a caixa **Ativar a gravação do dump** para ativar o aplicativo para gravar arquivos de dump de aplicativo.
5. Execute uma das seguintes ações:

   - Marque a caixa de seleção **Enviar arquivos de dump e de rastreamento para o Kaspersky** se você desejar que o aplicativo exiba uma solicitação na janela **Carregar informações do Suporte Técnico ao servidor**

para enviar arquivos de rastreio e dump para a Kaspersky para análise das causas do travamento do aplicativo no próximo início do aplicativo.

- Caso contrário, desmarque a caixa de seleção **Enviar arquivos de dump e de rastreamento para o Kaspersky**.

6. Clique em **OK** na janela **Modo operacional**.
7. Para salvar as alterações, clique no botão **Salvar** na janela principal do aplicativo.

Enviar arquivos para o servidor do Suporte Técnico

Os Arquivos que contêm informações sobre o sistema operacional, arquivos de rastreio e arquivos de dump devem ser enviados a peritos do Suporte técnico da Kaspersky.

Para enviar arquivos ao Servidor do Suporte Técnico:

1. Reinicie o Kaspersky Endpoint Security depois de qualquer mau funcionamento na sua operação.

   Isso abre-se a janela **A inicialização anterior do aplicativo falhou**.

   A janela **A inicialização anterior do aplicativo falhou** será aberta cada vez que o Kaspersky Endpoint Security for iniciado (inclusive depois de reiniciar o computador) até que você envie os arquivos de dump e arquivos de rastreio ao Suporte Técnico ou clique no botão**Não enviar**.

2. Na janela **A inicialização anterior do aplicativo falhou**, abra a lista de arquivos gerados **clicando aqui**.
3. Marque as caixas de seleção ao lado daqueles arquivos que você quer enviar ao Suporte Técnico.
4. Clique no botão **Exibir texto da Declaração**.

   A janela **Declaração Sobre Provisionamento de Dados** é aberta.

5. Leia o texto da Declaração Sobre Provisionamento de Dados e clique no botão **Fechar**.
6. Na janela **A inicialização anterior do aplicativo falhou**, marque a caixa de seleção **Concordo com a Declaração Sobre Provisionamento de Dados**.
7. Clique no botão **Enviar**.

   É exibida a janela **Número da solicitação**.

8. Na janela **Número da solicitação**, especifique o número que foi atribuído à sua solicitação quando você contatou o Suporte Técnico por meio da Kaspersky CompanyAccount.
9. Clique em **OK**.

Os arquivos de dados selecionados são compactados e enviados ao servidor do Suporte Técnico.

Ativar e desativar a proteção de arquivos de dump e arquivos de rastreio

Os arquivos de dump e os arquivos de rastreio contêm informações sobre o sistema operacional, bem como dados confidenciais do usuário. Para impedir o acesso não autorizado a tais dados, você pode ativar a proteção de arquivos de dump e arquivos de rastreio.

Se a proteção de arquivos de dump e de rastreamento for ativada, os arquivos poderão ser acessados pelos seguintes usuários:

- Os arquivos de dump podem ser acessados pelo administrador de sistema e administrador local, e pelo usuário que ativou a escrita de arquivos de dump e arquivos de rastreio.
- Os arquivos de rastreio podem ser acessados somente pelo administrador do sistema e administrador local.

Ativar ou desativar a proteção de arquivos de dump e arquivos de rastreio:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Configurações avançadas** à esquerda.

   As configurações do aplicativo são exibidas na parte direita da janela.
3. Na seção **Modo operacional**, clique no botão **Configurações**.

   A janela **Modo operacional** é exibida.
4. Execute uma das seguintes ações:
   - Marque a caixa de seleção **Ativar proteção de arquivos de dump e de rastreamento** se desejar ativar a proteção.
   - Limpe a caixa de seleção **Ativar proteção de arquivos de dump e de rastreamento** se desejar desativar a proteção.
5. Clique em **OK** na janela **Modo operacional**.
6. Para salvar as alterações, clique no botão **Salvar** na janela principal do aplicativo.

Os arquivos de dump e os arquivos de rastreamento que foram escritos enquanto a proteção foi ativada permanecem protegidos até depois que essa função é desativada.

Glossário

Agente de Autenticação

Uma interface para passar o processo de autenticação para acessar discos rígidos criptografados e carregar o sistema operacional após a criptografia do disco rígido.

Agente de Rede

Um componente do Kaspersky Security Center que permite a interação entre o Servidor de Administração e os aplicativos da Kaspersky que estão instalados em um nó de rede específico (estação de trabalho ou servidor). Este componente é característico para todos os aplicativos da Kaspersky que executam no Windows. As versões dedicadas do Agente de Rede são destinadas a aplicativos que executam em outros sistemas operacionais.

Alarme falso

O alarme falso ocorre quando o aplicativo da Kaspersky informa que um arquivo não infectado está infectado porque a assinatura do arquivo é similar a do vírus.

Análise de Assinaturas

Uma tecnologia de detecção de ameaça que usa bancos de dados do Kaspersky Endpoint Security, que contém descrições de ameaças conhecidas e os métodos para erradicá-las. A proteção por meio da análise de assinaturas fornece um nível de segurança minimamente aceitável. Seguindo as recomendações dos especialistas da Kaspersky, este método está sempre ativado.

Análise Heurística

A tecnologia foi desenvolvida para detectar ameaças que não podem ser detectadas usando a versão atual dos bancos de dados do aplicativo Kaspersky. Detecta arquivos que podem estar infectados por um vírus desconhecido ou por uma nova variedade de um vírus conhecido.

Arquivo compactado

Um ou vários arquivos foram compactados em um único arquivo compactado. Um aplicativo especializado chamou um arquivador que é necessário para compactar e descompactar dados.

Arquivo infectado

Arquivo que contém código malicioso (o código de malware conhecido foi detectado durante a verificação do arquivo). A Kaspersky não recomenda a utilização de tais objetos, pois eles podem infectar o computador.

Arquivo infectável

Um arquivo que, devido a sua estrutura ou ao seu formato, pode ser usado por invasores como um "contêiner" para armazenar e difundir um código malicioso. Normalmente, são arquivos executáveis com extensões como .com, .exe e .dll. Existe um risco bastante alto de intrusão de código malicioso nesses arquivos.

Arquivo provavelmente infectado

Um arquivo que contenha um código modificado de um vírus conhecido ou um código que seja semelhante ao de um vírus, mas que ainda não seja conhecido pela Kaspersky. Os arquivos provavelmente infectados são detectados pelo Analisador Heurístico.

Assunto de certificado

O titular de uma chave privada ligada a um certificado. Pode ser um usuário, aplicativo, qualquer objeto virtual, computador ou serviço.

Atualização

Procedimento de substituição ou adição de novos arquivos (bancos de dados ou módulos do aplicativo) que são recuperados dos servidores de atualização da Kaspersky.

Backup

Um armazenamento especial para cópias de backup dos arquivos que são criados antes da desinfecção ou exclusão ser tentada.

Banco de dados de endereços da Web maliciosos

Lista de endereços da Web cujo conteúdo é considerado possivelmente perigoso. Essa lista é criada pelos especialistas da Kaspersky. Ela é atualizada periodicamente, sendo incluída no Kit de distribuição do aplicativo da Kaspersky.

Banco de dados dos endereços da web de phishing

Lista de endereços da web os quais os especialistas da Kaspersky determinaram que estão relacionados com ataques de phishing. O banco de dados é atualizado periodicamente e faz parte do Kit de distribuição do aplicativo da Kaspersky.

Bancos de dados do Antivírus

Os bancos de dados contêm informações sobre ameaças à segurança do computador conhecidas da Kaspersky na data de publicação do banco de dados de antivírus. As assinaturas de banco de dados de antivírus ajudam a detectar código malicioso em objetos verificados. Os bancos de dados de antivírus são criados pelos peritos da Kaspersky e atualizados a cada hora.

Certificado

Documento eletrônico que contém a chave privada e informações sobre o proprietário da chave e o escopo de chave, e que confirma que a chave pública pertence ao proprietário. O certificado deve ser assinado pelo centro de certificado que o emitiu.

Certificado de licença

Um documento que a Kaspersky transfere para o usuário com o arquivo de chave ou código de ativação. Ele contém informações sobre a licença concedida ao usuário.

Chave adicional

Chave que certifica o direito de uso do aplicativo, mas que não está em uso atualmente.

Chave ativa

Chave que está atualmente em uso pelo aplicativo.

Conector do Agente de Rede

Funcionalidade do aplicativo que conecta o aplicativo com o Agente de rede. O Agente de rede ativa a administração remota do aplicativo através do Kaspersky Security Center.

Configurações da tarefa

Configurações do aplicativo específicas de cada tipo de tarefa.

Configurações do aplicativo

Configurações do aplicativo que são comuns a todos os tipos de tarefas e regulam a operação do aplicativo, como por exemplo configurações desempenho do aplicativo, configurações de relatório e configurações de Backup.

Correção

Uma pequena adição ao aplicativo que corrige bugs descobertos durante o funcionamento do aplicativo ou instala atualizações.

Desinfecção

Um método de processar objetos infectados que resulta em recuperação total ou parcial de dados. Nem todos os objetos infectados podem ser desinfectados.

Emissor de certificado

O centro de certificado que emitiu o certificado.

Escopo da verificação

Objetos que o Kaspersky Endpoint Security verifica ao executar uma tarefa de verificação.

Escopo de proteção

Objetos que estão sendo constantemente verificados pela proteção antivírus ao serem executados. O escopo de proteção de componentes diferentes tem propriedades diversas.

Forma normal de endereço de um recurso da Web

O formato normalizado do endereço de um recurso da Web é uma representação textual de um endereço do recurso da Web que é obtido por meio da normalização. A normalização é o processo em que a representação textual do endereço de um recurso da Web é alterada segundo regras específicas (por exemplo, exclusão de login, senha e porta de conexão HTTP da representação textual do endereço do recurso da Web; além disso, o endereço do recurso da Web altera os caracteres que estão em maiúsculas para minúsculas).

Para fins de proteção antivírus, o objetivo da normalização de endereços do recurso da Web é evitar a verificação de endereços de sites, que podem diferir em sintaxe, embora sejam fisicamente equivalentes, mais de uma vez.

Exemplo:

Endereço não normalizado: www.Exemplo.com\.

Endereço normalizado: www.exemplo.com\.

Gerenciador de Arquivos Portátil

Este é um aplicativo que fornece uma interface para trabalhar com arquivos criptografados em unidades removíveis quando nenhuma funcionalidade de criptografia está disponível no computador.

Grupo de administração

Um conjunto de computadores que compartilham funções comuns e um conjunto de aplicativos da Kaspersky instalados neles. Os dispositivos são colocados em grupos a fim de que possam ser gerenciados convenientemente como uma única unidade. Um grupo poderá incluir outros grupos. É possível criar políticas de grupo e tarefas de grupo, para cada aplicativo instalado no grupo.

Impressão digital do certificado

Informações usadas para identificar uma chave de certificado. Uma impressão digital é criada aplicando uma função hash criptografada ao valor da chave.

Lista negra de endereços

Uma lista de endereços de e-mail dos quais todas as mensagens de e-mail recebidas são bloqueadas pelo aplicativo da Kaspersky, seja qual for o conteúdo da mensagem.

Máscara de arquivo

Representação de um nome de arquivo e extensão usando curingas.

As máscaras de arquivos podem conter caracteres que são permitidos em nomes de arquivos, incluindo curingas:

- ***** – Substitui qualquer caractere igual ou superior a zero.
- **?** – Substitui um caractere individual.

Observe que o nome e a extensão são sempre separados por um ponto.

Módulo de plataforma confiável

Um microchip desenvolvido para fornecer funções básicas relacionadas à segurança (por exemplo, para guardar chaves de criptografia). Um Módulo de Plataforma Confiável normalmente é instalado na placa mãe do computador e interage com todos os outros componentes do sistema via barramento de hardware.

Módulos do aplicativo

Arquivos que estão incluídos no arquivo setup do aplicativo, que implementa a funcionalidade principal do aplicativo. Um módulo executável separado corresponde a cada tipo de tarefa que é executada pelo aplicativo (Proteção em tempo real, Verificação por demanda, Atualização). Quando executar verificação completa do computador na janela principal do aplicativo, é iniciado o módulo desta tarefa.

Mover arquivos para a Quarentena

Método para administrar um arquivo provavelmente infetado em que o acesso ao arquivo é bloqueado e o arquivo é movido da pasta de origem para a pasta Quarentena, onde é mantido em forma criptografada para eliminar a ameaça de infecção.

Objeto OLE

Um arquivo anexado ou um arquivo que está incorporado em outro arquivo. Os aplicativos Kaspersky permitem a verificação da existência de vírus em objetos OLE. Por exemplo, se você inserir uma tabela do Microsoft Office Excel® em um documento do Microsoft Office Word, a tabela será verificada como um objeto OLE.

Phishing

Um tipo de fraude na Internet na qual as mensagens de e-mail são enviadas com o objetivo de roubar dados confidenciais, com maior frequência os dados financeiros.

Programas maliciosos

O código Programa que usa uma espécie de vulnerabilidade no sistema ou software. Os programas maliciosos muitas vezes são usados para instalar o malware no computador sem o conhecimento do usuário.

Quarentena

O Kaspersky Endpoint Security coloca arquivos provavelmente infectados nesta pasta. Arquivos em quarentena são armazenados em formato criptografado.

Serviço de rede

Estabelece parâmetros que definem a atividade de rede. Para esta atividade de rede, você pode criar uma regra de rede que regula a operação do Firewall.

Servidor de Administração

Um componente do Kaspersky Security Center que armazena centralmente informações sobre todos os aplicativos da Kaspersky instalados dentro da rede corporativa. Ele pode ser utilizado para gerenciar esses aplicativos.

Tarefa

Funções executadas pelo aplicativo da Kaspersky como tarefas, por exemplo: Proteção de arquivo em tempo real, Verificação Completa de dispositivo, Atualização de banco de dados.

Informações sobre o código de terceiros

Informações adicionais sobre o código de terceiros são mantidas em legal_notices.txt, na pasta de instalação do aplicativo.

Notificações de marcas comercias

As marcas registradas e as marcas de serviço são propriedade de seus respectivos proprietários.

Adobe, Acrobat e Shockwave são marcas comerciais ou marcas registradas da Adobe Systems Incorporated nos EUA e/ou em outros países.

Mac e FireWire são marcas comerciais da Apple Inc. registradas nos Estados Unidos e em outros países.

AutoCAD é uma marca comercial ou a marca registrada comercial da Autodesk, Inc. e/ou as suas filiais/subsidiárias nos Estados Unidos e em outros países.

A marca nominativa Bluetooth e seu logotipo são propriedade da Bluetooth SIG, Inc.

Borland é uma marca registrada ou a marca registrada comercial de Borland Software Corporation nos Estados Unidos e outros lugares.

Citrix and Citrix Provisioning Services são marcas registradas da Citrix Systems, Inc. e/ou as suas filiais registradas no escritório de patentes dos Estados Unidos e outros países.

dBase é uma marca comercial da dataBased Intelligence, Inc.

EMC e SecurID são as marcas registradas da EMC Corporation ou marcas registradas comerciais da EMC Corporation nos Estados Unidos e outros países.

ICQ é uma marca comercial e/ou marca de serviço da ICQ LLC.

Intel e Pentium são marcas comerciais da Intel Corporation registradas nos EUA e em outros países.

Logitech é uma marca registrada ou a marca registrada comercial da Logitech Company nos Estados Unidos e outros países.

Mail.Ru é uma marca registrada da Mail.Ru. LLC.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell e Surface são marcas comerciais da Microsoft Corporation, registradas nos EUA e em outros países.

Mozilla e Thunderbird são marcas comerciais do Mozilla Foundation.

Novell é uma marca comercial da Novell Inc. registrada nos EUA e em outros países.

Java e JavaScript é uma marca registrada da Oracle Corporation e/ou suas afiliadas.

SafeNet é a marca registrada comercial da SafeNet, Inc.

UNIX é uma marca comercial registrada nos Estados Unidos e em outros países e é usada de acordo com a licença de X/Open Company Limited.