kaspersky

Kaspersky Endpoint Security for Mac

© 2026 AO Kaspersky Lab

Índice

Visão geral do Kaspersky Endpoint Security

Novidades desta versão

Comparação entre as funções do Kaspersky Endpoint Security, dependendo da ferramenta de gerenciamento do Kaspersky Security Center

Instale e desinstale o aplicativo

- Kit de distribuição
- Requisitos de hardware e software
- Preparar para a instalação
- Instalar o Kaspersky Endpoint Security
- Preparar o aplicativo para uso
- Desinstalar o Kaspersky Endpoint Security

Iniciar o aplicativo pela primeira vez

Interface do aplicativo Kaspersky Endpoint Security

- Janela principal do aplicativo
- Ícone do Kaspersky Endpoint Security
- Janela de ajustes do aplicativo

Sobre as notificações

Licenças do aplicativo Kaspersky Endpoint Security

- Sobre o Contrato de Licença de Usuário Final
- Sobre a licença
- Sobre a assinatura
- Sobre o certificado de licença
- Sobre a chave
- Sobre o código de ativação
- Sobre o arquivo de chave
- Sobre a coleta de dados
- Ativar o Kaspersky Endpoint Security
- Exibir informações da licença
- Gerenciar licenças e assinaturas
- Comparação da funcionalidade do aplicativo para estações de trabalho conforme o tipo de licença

Executar tarefas comuns

- Abrir e sair do aplicativo
- Exibir o status de proteção do computador
- Exibição do status operacional dos componentes instalados
- Desativar e retomar a proteção do computador
- Usar o Centro de Proteção
- Executar tarefas de verificação
- Configurar o início automático de uma tarefa de verificação agendada
- Atualizar os bancos de dados do aplicativo
- O que fazer se o acesso ao arquivo estiver bloqueado
- Restaurar um arquivo que foi excluído ou desinfectado pelo aplicativo
- Exibir o relatório de funcionamento do aplicativo
- O que fazer se forem exibidas janelas de notificação

Configuração avançada do aplicativo
- Escopo da proteção do computador
- Proteção Contra Ameaças ao Arquivo
- Proteção Contra Ameaças da Web
- Proteção Contra Ameaças ao Correio
- Proteção Contra Ameaças à Rede
- Firewall
- Detecção de Comportamento
- Verificação
- Tarefas de atualização
- Tarefas locais
  - Tarefa de verificação dos discos externos
- Backup
- Relatórios
- Managed Detection and Response
- Endpoint Detection and Response Expert (on-premise)
- Endpoint Detection and Response Optimum
  - Integração com o Endpoint Detection and Response Optimum
  - Verificar indicadores de comprometimento
  - Mover arquivo para a Quarentena
  - Obter arquivo
  - Excluir arquivo
  - Iniciar processo
  - Encerrar processo
  - Prevenção de execução
  - Isolamento da rede de computadores
  - Cloud Sandbox
- Criptografia de disco FileVault
- Proteção por senha
- Prevenção de Exploits
- Mecanismo de Remediação
- Controle da Web
- Controle de Dispositivos

Participar na Kaspersky Security Network

Verifique a integridade dos componentes do aplicativo

Gerenciar o aplicativo por meio do Console de Administração do Kaspersky Security Center
- Implantar o Kaspersky Endpoint Security em uma rede corporativa
- Atualizar o Kaspersky Endpoint Security da versão 11.1 ou posterior para a versão 12.2.1
- Preparo para a instalação remota do Kaspersky Endpoint Security
  - Instalar o plugin de administração do Kaspersky Endpoint Security
  - Instalar o Agente de Rede localmente
  - Instalar o Agente de Rede usando o Apple Remote Desktop
  - Instalar o Agente de Rede usando o Kaspersky Security Center
  - Instalar o Agente de Rede usando o protocolo SSH
  - Desinstalar o Agente de Rede localmente

- Gerenciar o Agente de Rede a partir da linha de comando
  - Iniciar/parar o Agente de Rede em um computador remoto
  - Verificar a conexão entre um computador cliente e o Servidor de Administração manualmente. Utilitário Klnagchk
  - Conectar um computador remoto ao Servidor de Administração manualmente. Utilitário klmover
  - Desinstalar o Agente de Rede
- Instalar e desinstalar o Kaspersky Endpoint Security
  - Instalar o aplicativo usando o protocolo SSH
  - Instalar o aplicativo usando o Kaspersky Security Center
  - Criar um pacote de instalação
  - Desinstalar o aplicativo usando o Kaspersky Security Center
- Iniciar e parar o aplicativo via Kaspersky Security Center
- Criar e gerenciar tarefas
  - Criar tarefas
  - Iniciar e parar tarefas manualmente
  - Tarefas de importação e exportação
  - Exibir tarefas
  - Gerenciar configurações específicas da tarefa
- Criar e gerenciar políticas
  - Criar uma política
  - Exibir a lista de políticas
  - Definir configurações de políticas
  - Alterar o status da política
  - Exportar uma política para um arquivo KLP
  - Importar uma política de um arquivo KLP
- Criar e gerenciar perfis da política
- Gerar um relatório sobre objetos detectados
- Obter uma chave de recuperação para uma unidade criptografada

Administração remota do aplicativo por meio do Web Console e do Kaspersky Security Center Cloud Console

- Instalar o plug-in da web do Kaspersky Endpoint Security
- Criar uma política
  - Proteção contra ameaças ao host
    - Configure o componente Proteção Contra Ameaças ao Arquivo
    - Configure a Verificação de Unidades Removíveis
    - Configuração da Detecção de Comportamento
    - Configuração do Anti-Cryptor
    - Configuração do componente Prevenção de Exploits
    - Configuração do componente Mecanismo de Remediação
  - Comunicação e Proteção da Web
    - Configurar Proteção Contra Ameaças ao Correio
    - Configuração do componente Proteção Contra Ameaças da Web
    - Configure a Proteção Contra Ameaças à Rede
    - Configure o componente Firewall
  - Controles de Segurança
    - Configuração do componente Controle de Dispositivos
    - Configuração do componente Controle da Web
  - Criptografia de Dados

- Configurações gerais
  - Configurações de detecção
  - Kaspersky Security Network
  - Interação do usuário
  - Autodefesa
  - Desempenho
  - Relatórios e armazenamento
  - Configurações de rede
  - Configurações de telemetria
  - Configurações do evento
  - Configurações de atualização
- Agentes integrados
  - Configurar o Managed Detection and Response
  - Configuração do Endpoint Detection and Response
  - Configure o Endpoint Detection and Response Expert (on-premise)
- Criar tarefas
  - Definir as configurações da tarefa de Verificação
  - Definir as configurações da tarefa Adicionar chave
  - Configurar a tarefa de Atualização
- Obter uma chave de recuperação para uma unidade criptografada

Gerenciar o aplicativo pela linha de comando

- Exibir a ajuda da linha de comando
- Executar verificação de malware
- Atualizar o aplicativo
- Reverter a última atualização
- Iniciar/parar um componente ou uma tarefa
- Exibir status e estatísticas de um componente ou de uma tarefa
- Exportar as configurações de proteção
- Ativar o aplicativo
- Instale a extensão do sistema
- Defina as conexões de rede
- Remover as chaves de licença
- Códigos de retorno da linha de comando
- Encerrar o aplicativo
- Desinstalar o aplicativo
- Comandos de gerenciamento de Detection and Response
  - Gerenciar a prevenção de execução
  - Gerenciar o isolamento de rede

Entrar em contato com o Suporte Técnico

- Como obter Suporte Técnico
- Suporte Técnico via Kaspersky CompanyAccount
- Adquirir informações para Suporte Técnico
- Usar um arquivo de rastreamento
- Criar um arquivo de rastreamento

Fontes de informação sobre o aplicativo

Apêndices
- Problemas e limitações conhecidos
- Problemas corrigidos
- Lista de objetos verificados por extensão
- Máscaras nos caminhos para arquivos e pastas
- Requisitos do arquivo IOC
- Interpretadores de script compatíveis com a Prevenção de execução
- Como adicionar o certificado da Kaspersky Endpoint Security ao armazenamento de certificados do Mozilla Firefox
- Configurações de rede para interação com serviços externos

Informações sobre código de terceiros

Notas sobre marcas comerciais

Visão geral do Kaspersky Endpoint Security

O aplicativo Kaspersky Endpoint Security protege os computadores que executam o macOS contra malware e outras ameaças à segurança do computador.

Proteção Contra Ameaças ao Arquivo

A Proteção contra Ameaças ao Arquivo protege o sistema de arquivos do computador em tempo real ao interceptar e analisar quaisquer tentativas de acessar os arquivos. Saiba mais.

Proteção Contra Ameaças da Web

A Proteção Contra Ameaças da Web protege as informações enviadas e recebidas por seu computador através dos protocolos HTTP e HTTPS no Safari, Google Chrome™ e Firefox™. Saiba mais.

Proteção Contra Ameaças ao Correio

A Proteção Contra Ameaças ao Correio verifica os anexos de mensagens de e-mail recebidas e enviadas em busca de malware e outras ameaças. O componente protege o computador usando bancos de dados antimalware, o serviço em nuvem da Kaspersky Security Network e a análise heurística. Saiba mais.

Proteção Contra Ameaças à Rede

A Proteção contra Ameaças à Rede evita invasões no sistema operacional. Esse componente protege contra hackers (que usam a verificação de porta e ataques de força bruta) e contra os malwares que eles instalam (incluindo malwares que tentam enviar dados pessoais aos criminosos). Saiba mais.

Firewall

O Firewall bloqueia as conexões não autorizadas com o computador durante o trabalho na Internet ou rede local. Isso permite proteger sua LAN contra roubo de identidade e outros ataques. O componente oferece proteção ao computador com a ajuda de bancos de dados antimalware, do serviço em nuvem da Kaspersky Security Network e de regras de rede predefinidas. Saiba mais.

Detecção de Comportamento

O componente Detecção de Comportamento recebe informações sobre as ações dos aplicativos no computador para fornecê-las a outros componentes de proteção para melhorar o desempenho. Ele também executa a ação selecionada como uma resposta à atividade de malware. Saiba mais.

Prevenção de Exploits

O componente de Prevenção de Exploits detecta o código do programa que aproveita as vulnerabilidades no computador para explorar privilégios de administrador ou executar atividades maliciosas. Saiba mais.

Mecanismo de Remediação

O Mecanismo de Remediação permite que o Kaspersky Endpoint Security desfaça ações executadas por Malwares no sistema operacional. Saiba mais.

Verificação

O aplicativo Kaspersky Endpoint Security detecta e neutraliza malware e outras ameaças de segurança ao computador sob demanda no escopo da verificação especificado. O Kaspersky Endpoint Security pode executar uma verificação completa do computador, uma verificação rápida das áreas críticas e uma verificação do escopo especificado. Saiba mais.

Atualização

O Kaspersky Endpoint Security atualiza os bancos de dados e módulos do aplicativo a partir dos servidores de atualização Kaspersky, dos pontos de distribuição ou de outras fontes especificadas pelo administrador do sistema e cria cópias de backup de todos os arquivos atualizados para permitir a reversão da última atualização. Saiba mais.

Backup

O Kaspersky Endpoint Security cria uma cópia de backup dos arquivos infectados antes de qualquer tentativa de desinfecção ou exclusão, possibilitando a restauração deles. Saiba mais.

Relatórios

O Kaspersky Endpoint Security gera relatórios sobre os eventos e as ações que envolvem os componentes do aplicativo. Saiba mais.

Notificações

O Kaspersky Endpoint Security usa notificações para informar você sobre certos eventos na operação do Kaspersky Endpoint Security. As notificações podem ser acompanhadas de alertas sonoros. Saiba mais.

Centro de Proteção

O Kaspersky Endpoint Security exibe mensagens do status da proteção no Centro de Proteção. O Centro de Proteção exibe informações sobre o status da proteção do computador e sobre como eliminar problemas e ameaças à segurança do computador. Saiba mais.

Gerenciamento remoto do aplicativo via Kaspersky Security Center

Você pode gerenciar remotamente a proteção de computadores com o Kaspersky Endpoint Security instalado: receber informações sobre o status atual da proteção do computador, corrigir problemas remotamente, responder a ameaças à segurança, ativar ou desativar componentes de proteção (Proteção contra Ameaças ao Arquivo, Proteção contra Ameaças da Web, Proteção contra Ameaças à Rede, Detecção de Comportamento), ativar ou desativar o Controle da Web, o Managed Detection and Response, o Endpoint Detection and Response e o Endpoint Detection and Response Expert (on-premise), executar tarefas de verificação, atualizar bancos de dados do aplicativo, executar a criptografia de disco e gerenciar licenças e assinaturas do Kaspersky Endpoint Security. É possível usar as seguintes ferramentas para gerenciar o Kaspersky Endpoint Security:

- Console de Administração do Kaspersky Security Center. Saiba mais.
- Kaspersky Security Center Web Console e Cloud Console. Saiba mais.

Nota: a funcionalidade suportada pelo Kaspersky Endpoint Security depende da ferramenta de gerenciamento usada.

Criptografia de disco FileVault

O Kaspersky Endpoint Security permite que a criptografia do FileVault seja gerenciada remotamente. A criptografia impede que usuários não autorizados acessem dados confidenciais armazenados no disco de inicialização do computador do usuário.

Controle da Web

Você pode gerenciar remotamente o acesso a sites visitados pelos usuários. Você pode permitir ou bloquear o acesso a endereços ou grupos de endereços específicos da Web. Além disso, você pode permitir ou bloquear o acesso a determinadas categorias de sites com base em conteúdo. Saiba mais.

Controle de Dispositivos

O Controle de Dispositivos gerencia o acesso dos usuários aos dispositivos instalados ou conectados ao computador. Isso permite proteger o computador contra infecções quando esses dispositivos estão conectados e evitar a perda ou vazamento de dados. Saiba mais.

Managed Detection and Response

O componente Managed Detection and Response fornece interação com o serviço Kaspersky Managed Detection and Response que detecta e elimina constantemente as ameaças à segurança direcionadas à sua organização. Saiba mais.

Endpoint Detection and Response

O componente Endpoint Detection and Response facilita a interação com a solução Kaspersky Endpoint Detection and Response. Esta solução combina a detecção automática de ameaças com a capacidade de reagir a essas ameaças para neutralizar ataques avançados, incluindo novos exploits, ransomware, ataques sem arquivo, bem como métodos que usam ferramentas de sistema legítimas. Saiba mais.

Endpoint Detection and Response Expert (on-premise)

O componente Endpoint Detection and Response Expert (on-premise) facilita a interação com a solução Kaspersky Anti Targeted Attack Platform. Essa solução detecta prontamente as ameaças avançadas, como ataques direcionados, ameaças persistentes avançadas, ataques de dia zero e outras. Saiba mais.

Novidades desta versão

Esta Ajuda aplica-se ao Kaspersky Endpoint Security for Mac versão 12.2.1.

O Kaspersky Endpoint Security oferece os seguintes aprimoramentos e novos recursos:

- O novo macOS 27 Golden Gate agora é compatível.
- A interface de gerenciamento de políticas no Web Console foi atualizada. A estrutura de seções da política foi alterada para garantir consistência com as interfaces dos plug-ins do Kaspersky Endpoint Security for Windows e Linux.
- Agora, você pode visualizar quais modificações foram feitas em uma política ao longo de um determinado período, além de salvar as informações sobre essas modificações em um arquivo.
- Adicionamos novos componentes: Proteção Contra Ameaças ao Correio, Controle de Dispositivos, Firewall, Mecanismo de Remediação e Prevenção de Exploits.
- Agora você pode ativar o componente Managed Detection and Response a partir do aplicativo Kaspersky Endpoint Security.
- Melhoramos a visibilidade das ações de resposta nos detalhes do alerta.
- Agora é possível gerenciar o componente Detecção de Comportamento no Web Console.
- Adicionamos resumos aos alertas.
- Agora uma notificação é enviada para avisar que um objeto é um sistema crítico antes que qualquer ação de resposta seja realizada.
- Agora é possível editar arquivos IOC diretamente no Web Console ao criar ou editar as configurações da tarefa de Verificação de IOC.
- Agora é possível mover os objetos detectados para a Quarentena dos detalhes do alerta.
- Adicionamos avisos para ações restritas na tarefa de Isolamento de rede.
- Correções gerais de erros e melhorias.

Comparação entre as funções do Kaspersky Endpoint Security, dependendo da ferramenta de gerenciamento do Kaspersky Security Center

A funcionalidade suportada pelo Kaspersky Endpoint Security depende da ferramenta de gerenciamento usada (veja a tabela abaixo).

É possível usar as seguintes ferramentas para gerenciar o Kaspersky Endpoint Security:

- Console de Administração do Kaspersky Security Center. Um snap-in do Console de Gerenciamento Microsoft (MMC) instalado na estação de trabalho do administrador do Kaspersky Security Center.
- Kaspersky Security Center Web Console. Um componente do Kaspersky Security Center instalado no Servidor de Administração. É possível trabalhar com o Web Console usando um navegador em qualquer computador que tenha acesso ao Servidor de Administração.
- Kaspersky Security Center Cloud Console. A versão na nuvem do Kaspersky Security Center.

Comparação de recursos do Kaspersky Endpoint Security

Recurso	Kaspersky Security Center		
	Console de Administração	Web Console	Cloud Console
Proteção Avançada Contra Ameaças			
Kaspersky Security Network	✓	✓	✓
Detecção de Comportamento	✓	✓	
Prevenção de Exploits	✓	✓	
Mecanismo de Remediação	✓	✓	
Proteção Essencial Contra Ameaças			
Proteção Contra Ameaças ao Arquivo	✓	✓	✓
Proteção Contra Ameaças da Web	✓	✓	✓
Proteção Contra Ameaças à Rede	✓	✓	✓
Proteção Contra Ameaças ao Correio	✓	✓	
Firewall	✓	✓	
Controles de Segurança			
Controle da Web	✓	✓	✓
Controle de Dispositivos	✓	✓	
Criptografia de Dados			
Criptografia de disco FileVault	✓	✓	✓
Chave de Recuperação	✓	✓	✓
Detection and Response			
Managed Detection and Response	✓	✓	✓
Endpoint Detection and Response		✓	

Recurso	Kaspersky Security Center		
	Console de Administração	Web Console	Cloud Console
Endpoint Detection and Response Expert (on-premise)	✓	✓	✓
Tarefas			
Adicionar chave	✓	✓	✓
Atualização	✓	✓	✓
Verificação Rápida	✓	✓	
Reversão	✓	✓	✓
Verificação	✓	✓	✓

Instale e desinstale o aplicativo

Kit de distribuição

O kit de distribuição inclui o pacote de instalação do Kaspersky Endpoint Security, que contém os seguintes arquivos:

- Arquivos necessários para instalar o aplicativo de qualquer um dos modos disponíveis.
- O arquivo license_<loc>.txt com o Contrato de Licença de Usuário Final.

  O Contrato de Licença de Usuário Final especifica os termos de uso do aplicativo.

Descompacte o pacote de instalação compactado para acessar os arquivos incluídos.

Requisitos de hardware e software

O Kaspersky Endpoint Security tem os seguintes requisitos de hardware e software:

- Tipo de processador: Intel, Apple Silicon
- 4 GB de memória (RAM)
- 5 GB de espaço livre em disco
- macOS 14, 15, 26, 27
- Conexão com a Internet

Navegadores compatíveis:

- Safari
- Chrome
- Firefox

O Kaspersky Endpoint Security é compatível com as seguintes ferramentas de virtualização:

- Parallels Desktop 16 for Mac Business Edition ou posterior
- VMware Fusion™ 11.5 Professional
- VMware Fusion 12 Professional
- VMware Fusion 13 Pro

Perfis MDM podem ser implantados com os servidores Jamf e Apple. Se você usa outros servidores, consulte o artigo no site do Suporte Técnico (Base de conhecimento).

Você pode gerenciar o Kaspersky Endpoint Security remotamente via Kaspersky Security Center. O Kaspersky Security Center 14.2 ou posterior é necessário para gerenciar o Kaspersky Endpoint Security usando o plugin de administração para o Console de Administração do Kaspersky Security Center e o plugin da Web para o Kaspersky Security Center Web Console.

Nota: para gerenciar o Kaspersky Endpoint Security for Mac 12.2.1 pelo Kaspersky Security Center, é necessário instalar o Agente de Rede versão 15 nos computadores remotos.

Preparar para a instalação

Antes de instalar o aplicativo Kaspersky Endpoint Security no seu computador, recomenda-se fazer o seguinte:

- Assegure-se de que seu computador atenda aos requisitos de hardware e software.
- Remova o Kaspersky Internet Security for Mac ou outros aplicativos anti-malware para evitar conflitos de sistema e maximizar o seu desempenho.

Nota: antes de instalar o Kaspersky Endpoint Security remotamente, recomendamos que você baixe o arquivo comprimido KES_for_macOS11_and_later.zip do site de Suporte Técnico da Kaspersky e aplique o perfil de configuração KES_for_macOS11_and_later_profile.mobileconfig no computador cliente usando as ferramentas de gerenciamento remoto da Apple. Isso permitirá que o Kaspersky Endpoint Security obtenha os seguintes recursos: permissões para instalar a extensão de kernel e a extensão do sistema, acesso total ao disco e permissões para configurar conexões de rede. Para saber mais sobre o perfil de configuração e outras opções, visite o site do Suporte Técnico.

Instalar o Kaspersky Endpoint Security

Importante: os especialistas da Kaspersky recomendam instalar o Kaspersky Endpoint Security apenas de acordo com as descrições desta ajuda.

É possível instalar o Kaspersky Endpoint Security de uma das seguintes maneiras:

- Localmente usando o kit de distribuição baixado no site da Kaspersky.
- Remotamente usando Apple Remote Desktop
- Remotamente por meio do Console de Administração do Kaspersky Security Center.
- Remotamente por meio do Web Console ou do Kaspersky Security Center Cloud Console.

  Para obter informações detalhadas sobre a implementação de aplicativos da Kaspersky com o uso do Kaspersky Security Center Web Console, consulte a ajuda do Kaspersky Security Center. Para obter informações detalhadas sobre a implementação de aplicativos da Kaspersky usando o Kaspersky Security Center Cloud Console, consulte a Ajuda do Kaspersky Security Center Cloud Console.

Executar uma instalação padrão do Kaspersky Endpoint Security

1. Descompacte o arquivo comprimido ZIP do kit de distribuição.
2. Abra o arquivo comprimido .dmg a partir do conteúdo do arquivo descompactado.
3. Na janela que se abre, clique duas vezes em **Instalar o Kaspersky Endpoint Security**.

   O Assistente de Instalação do Kaspersky Endpoint Security é aberto.
4. Clique em **Instalar**.
5. Siga as etapas do Assistente de Instalação para concluir a instalação.

Quando a instalação for concluída, o Kaspersky Endpoint Security inicia automaticamente. Não é necessário reiniciar o seu computador.

Observação: se esse método de instalação for usado, os componentes Endpoint Detection and Response Expert (on-premise), Endpoint Detection and Response (Optimum) e Cloud Sandbox não serão instalados.

Executar uma instalação personalizada do Kaspersky Endpoint Security

1. Descompacte o arquivo comprimido ZIP do kit de distribuição.
2. Abra o arquivo comprimido .dmg a partir do conteúdo do arquivo descompactado.
3. Na janela que se abre, clique duas vezes em **Instalar o Kaspersky Endpoint Security**.

   O Assistente de Instalação do Kaspersky Endpoint Security é aberto.
4. Clique em **Personalizar**, marque ou desmarque as caixas de seleção ao lado dos componentes que você não deseja instalar e clique em **Continuar**.
5. Siga as etapas do Assistente de Instalação para concluir a instalação.

Quando a instalação for concluída, o Kaspersky Endpoint Security inicia automaticamente. Não é necessário reiniciar o seu computador.

Instalar o Kaspersky Endpoint Security remotamente usando o Apple Remote Desktop

1. No Mac, escolha o **menu Apple** > **Ajuste do Sistema** > **Geral** > **Compartilhamento**.
2. Marque a caixa de seleção **Gerenciamento Remoto**.
3. Em outro Mac que será o servidor, instale o Apple Remote Desktop. Para obter mais informações sobre o Apple Remote Desktop, consulte o Suporte da Apple.
4. Abra o Apple Remote Desktop.
5. Na janela **Área de Trabalho Remota**, clique à esquerda em **Verificador** e selecione os dispositivos nos quais deseja instalar o Kaspersky Endpoint Security.
6. Clique em **Instalar**.
7. No prompt de credenciais de administrador, insira um nome de administrador e uma senha e clique em **Adicionar**.

8. Clique em + e selecione o arquivo .dmg com o pacote de instalação do Kaspersky Endpoint Security.
9. Clique em **Instalar**.

A instalação do Kaspersky Endpoint Security inicia-se nos dispositivos selecionados.

Preparar o aplicativo para uso

Após a instalação do Kaspersky Endpoint Security, você pode fazer o seguinte:

- Ativar o Kaspersky Endpoint Security. Quando o aplicativo é ativado, o Kaspersky Endpoint Security começa a proteger seu computador e será possível atualizar regularmente os bancos de dados e módulos do aplicativo, executar tarefas de verificação de malware e enviar solicitações ao Suporte Técnico.

  > O componente Managed Detection and Response é ativado separadamente no Kaspersky Security Center Administration ou Web Console.

  Caso o componente Endpoint Detection and Response não seja compatível com sua licença atual, será necessário ativar separadamente o Kaspersky Endpoint Detection and Response.

- Avaliar o status de proteção do computador.
- Atualizar o Kaspersky Endpoint Security.
- Verificar se há malware no computador.

Desinstalar o Kaspersky Endpoint Security

1. Abra o arquivo DMG do kit de distribuição de aplicativos.
2. Na janela com o conteúdo do kit de distribuição, clique duas vezes em **Desinstalar o Kaspersky Endpoint Security**.

   O desinstalador do Kaspersky Endpoint Security é iniciado.
3. Na janela do desinstalador, clique em **Desinstalar**.
4. No prompt para as credenciais de administrador, insira um nome e uma senha de administrador e confirme que você deseja desinstalar o Kaspersky Endpoint Security.

   A desinstalação do Kaspersky Endpoint Security é iniciada.
5. Leia as informações sobre a conclusão da desinstalação e clique em **Encerrar** para encerrar o desinstalador.

O Kaspersky Endpoint Security foi desinstalado do seu computador. Não é necessário reiniciar o seu computador após desinstalar o aplicativo.

Iniciar o aplicativo pela primeira vez

O Kaspersky Endpoint Security inicia no computador logo após a instalação. Para proteger seu Mac imediatamente, o aplicativo solicita que você execute a configuração básica:

- Conceda as permissões necessárias ao Kaspersky Endpoint Security para proteger o seu Mac contra malwares, ataques de rede e ameaças da Internet.

  Para obter mais informações sobre as permissões que você está concedendo, clique em ?.

- Ativar o Kaspersky Endpoint Security.

Nota: é necessária uma conexão com a Internet para a configuração básica do Kaspersky Endpoint Security.

Iniciar o Kaspersky Endpoint Security pela primeira vez

1. Na janela **Proteção essencial**, execute as seguintes ações para garantir que a Proteção Contra Ameaças ao Arquivo e a Proteção Contra Ameaças da Web funcionem corretamente:

   - Se desejar que o aplicativo Kaspersky Endpoint Security funcione corretamente, permita que ele verifique todos os arquivos no seu Mac. Para fazer isso, clique em **Permitir**, ao lado do item **Acesso total ao disco**, e siga as instruções na tela.

   - Se você quiser que o Kaspersky Endpoint Security inspecione URLs e pacotes de rede antes que eles possam danificar seu Mac, instale a extensão do sistema. Para fazer isso, clique em **Instalar** ao lado do item **Extensão do sistema** e siga as instruções na tela.

   - Se quiser que a extensão do sistema funcione corretamente, permita a filtragem de conteúdo da rede. Para fazer isso, clique em **Permitir** ao lado do item **Filtragem de conteúdo da rede** e siga as instruções na tela.

   - Se quiser que o Kaspersky Endpoint Security procure por malware e ameaças da Internet no tráfego HTTPS criptografado, instale o certificado confiável. Para fazer isso, clique em **Instalar** ao lado do item **Certificado confiável** e siga as instruções na tela.

   Nota: o aplicativo Kaspersky Endpoint Security não funcionará corretamente sem que essas permissões sejam concedidas. Você deve conceder todas as permissões na janela **Proteção essencial**.

2. Clique em **Continuar**.

A janela principal do aplicativo é aberta.

Interface do aplicativo Kaspersky Endpoint Security

Janela principal do aplicativo

Abrir a janela principal do aplicativo

Na barra de menus, clique no ícone do aplicativo e escolha **Kaspersky Endpoint Security**.

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

A janela principal do aplicativo é dividida em duas partes:

- A parte esquerda contém a barra lateral, que permite navegar pelo aplicativo e acessar rapidamente suas principais funções.
- A parte central exibe os conteúdos da seção selecionada na barra lateral e permite gerenciar dados.

Barra lateral

A barra lateral da janela principal do aplicativo tem as seguintes opções:

Monitoramento	Clique para abrir a página **Monitoramento**, que fornece as informações relativas ao que o Kaspersky Endpoint Security está fazendo para proteger o computador.
Centro de Proteção	Clique para exibir o status de proteção do computador. Saiba mais.
Segurança	Clique para visualizar o status operacional dos componentes instalados. Saiba mais.
Verificação	Clique para gerenciar as tarefas de verificação. Saiba mais.
Atualização	Clique para gerenciar as tarefas de atualização. Saiba mais.
Licença	Clique para ativar o aplicativo ou exibir as informações sobre a licença. Saiba mais.

Controles da página **Monitoramento**

A página **Monitoramento** exibe o indicador de status da proteção, fornece as informações sobre o que o Kaspersky Endpoint Security está fazendo para proteger o computador, além de conter os seguintes controles.

Centro de Proteção	Informa sobre os problemas de proteção do computador. Saiba mais.
Relatórios	Permite exibir os eventos que ocorreram durante a operação do aplicativo, componentes individuais e tarefas. Saiba mais.
Backup	Permite exibir uma lista de cópias salvas de arquivos infectados que o aplicativo excluiu. Saiba mais. Saiba mais.

Detecção de ameaças	Permite exibir as informações sobre as tecnologias de detecção de ameaças aplicadas pelo Kaspersky Endpoint Security e o número de ameaças detectadas por essas tecnologias.
Kaspersky Security Network	Exibe o status da conexão entre o Kaspersky Endpoint Security e a Kaspersky Security Network, além das estatísticas globais da Kaspersky Security Network.

Ícone do Kaspersky Endpoint Security

Quando o Kaspersky Endpoint Security for instalado, o ícone do Kaspersky Endpoint Security aparecerá na barra de menus. Quando for ativado, o ícone do aplicativo mostra o status. Se o ícone do aplicativo estiver ativo (), significa que todos ou alguns do componentes de proteção estão ativados. Se o ícone do aplicativo estiver inativo ( ), significa que todos os componentes de proteção estão desativados.

Abrir o menu do ícone do aplicativo

Na barra de menus, clique no ícone do aplicativo.

Por padrão, o ícone do aplicativo sempre é exibido na barra de menus. Você pode remover o ícone do aplicativo da barra de menus.

Remover o ícone do aplicativo da barra de menus

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.
   É aberta a janela de ajustes do aplicativo.
2. Na guia Interface, na seção **Ícone do aplicativo**, desmarque a caixa de seleção **Exibir na barra de menus**.

Quando você abre a janela do aplicativo, o ícone do aplicativo também aparece no **Dock**.

No menu do ícone do aplicativo, você pode acessar a janela principal do aplicativo e executar as seguintes ações:

- Desativar a proteção do computador.
- Reiniciar a proteção do computador.
- Abrir o Centro de Proteção.
- Iniciar a Verificação Rápida.
- Executar uma atualização.
- Abrir a janela de configurações do aplicativo.
- Sair do Kaspersky Endpoint Security.

Janela de ajustes do aplicativo

Abrir a janela de configurações do aplicativo

Siga um destes procedimentos:

- Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.
- Na barra de menus, clique em **Kaspersky Endpoint Security** > **Ajustes**.
- Se o Kaspersky Endpoint Security estiver em execução, clique no ícone do aplicativo no **Dock** e escolha **Ajustes**.

É possível acessar rapidamente as configurações do aplicativo usando as seguintes guias na parte superior da janela de configurações:

- **Essencial**. Nesta guia, você pode ativar ou desativar a proteção do computador e definir as configurações de Proteção Contra Ameaças ao Arquivo, Proteção Contra Ameaças da Web e Proteção Contra Ameaças à Rede.
- **Verificação**. Nesta guia, você pode definir as configurações das tarefas de verificação e de inicialização de tarefas de verificação programadas.
- **Ameaças**. Nesta guia, você pode selecionar as categorias de objetos a serem detectadas, criar a Zona Confiável e configurar as configurações de Backup.
- **Avançado**. Use esta guia para optar por participar ou não da Kaspersky Security Network.
- **Atualização**. Nesta guia, você pode definir as configurações de atualização do aplicativo ou reverter para a versão anterior dos bancos de dados do aplicativo.
- **Interface**. Nesta guia, você pode definir as configurações para o ícone, as notificações e os relatórios do Kaspersky Endpoint Security e ativar ou desativar o registro de informações de depuração em um arquivo de rastreamento.

Ao usar o botão  , você pode impedir que usuários sem direitos de administrador editem as configurações do Kaspersky Endpoint Security. Este botão está localizado na parte inferior da janela de configurações do aplicativo. Para editar as configurações, você deve inserir as credenciais do administrador.

Clicar no botão ? abrirá a ajuda do Kaspersky Endpoint Security, que descreve todas as configurações na janela atual do aplicativo. Você também pode abrir o tópico de ajuda para a janela ativa do aplicativo selecionando **Abrir a Ajuda desta janela** no menu **Ajuda**.

Sobre as notificações

O Kaspersky Endpoint Security exibe notificações para informar sobre eventos do aplicativo. Dependendo da versão do sistema operacional instalado no computador, as notificações são exibidas na Central de Notificações do sistema operacional. A aparência das notificações depende das opções definidas nas configurações de Notificação do sistema operacional.

Os eventos do Kaspersky Endpoint Security são divididos em três tipos de acordo com sua importância:

- *Crítico* – eventos que apresentam uma ameaça perigosa à segurança do computador (detecção de objetos maliciosos, vulnerabilidades, problemas com o Kaspersky Endpoint Security). Os eventos críticos exigem sua atenção imediata. Recomendamos que você não desative as notificações sobre eventos críticos.

- *Importante* – eventos que não exigem a atenção imediata, mas que podem apresentar uma ameaça à segurança do computador no futuro.

- *Informativo* - eventos relatados para sua informação.

Desativar as notificações

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Interface**, na seção **Notificações**, desmarque a caixa de seleção Ativar notificações.

Ativar registro de eventos não críticos

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Interface**, na seção **Relatórios**, marque a caixa de seleção **Registrar eventos não críticos** para receber notificações sobre eventos informativos do Kaspersky Endpoint Security.

Independentemente de as notificações estarem ativadas ou desativadas, os relatórios do aplicativo incluem informações sobre eventos que ocorrem enquanto o Kaspersky Endpoint Security está em execução.

As notificações podem ser acompanhadas de alertas sonoros (por exemplo, notificações sobre um malware detectado). Você pode desativar o alerta sonoro.

O registro de eventos não críticos aumenta consideravelmente o tamanho total do arquivo de relatório. Observe que essa configuração se aplica apenas à Proteção Contra Ameaças ao Arquivo.

Desativar os alertas sonoros que acompanham as notificações

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Interface**, na seção **Notificações**, desmarque a caixa de seleção **Ativar sons de alerta ao detectar malware**.

Se uma ação for necessária em resposta a um evento, o Kaspersky Endpoint Security exibirá uma janela de notificações. Por exemplo, quando o aplicativo detecta um objeto malicioso, ele solicita que o usuário exclua ou desinfecte o objeto. A janela de notificações desaparece da tela somente depois que uma das ações for selecionada.

Licenças do aplicativo Kaspersky Endpoint Security

Sobre o Contrato de Licença de Usuário Final

O *Contrato de Licença de Usuário Final* (Contrato de Licença) é um contrato entre Você e a AO Kaspersky Lab que estipula os termos segundo os quais você pode utilizar o aplicativo.

Importante: leia com atenção o Contrato de Licença antes de começar a usar o aplicativo.

Você pode visualizar os termos do Contrato de Licença de Usuário Final das seguintes formas:

- Durante a instalação do Kaspersky Endpoint Security
- Ao ler o documento license.txt na pasta de instalação do aplicativo

Ao instalar o Kaspersky Endpoint Security, você confirma que entendeu e aceita os termos do Contrato de Licença de Usuário Final. Caso você não aceite os termos do Contrato de Licença de Usuário Final, cancele a instalação do Kaspersky Endpoint Security e não utilize o aplicativo.

Sobre a licença

A *licença* é um direito de uso temporário do Kaspersky Endpoint Security, concedida sob os termos do Contrato de Licença (Contrato de Licença de Usuário Final).

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

Os seguintes tipos de licença são fornecidos:

- *Avaliação*. Uma licença gratuita destinada a experimentar o aplicativo.

  Uma licença de avaliação geralmente tem um prazo curto. Quando uma licença de avaliação expira, todos os recursos do Kaspersky Endpoint Security serão desativados. Para continuar usando o aplicativo, será necessário adquirir uma licença comercial.

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

- *Comercial*. Uma licença paga.

  Quando uma licença comercial expira, os principais recursos do aplicativo são desativados. Para continuar usando o Kaspersky Endpoint Security, é necessário renovar a licença comercial. Após a expiração de uma licença comercial, você não pode continuar usando o aplicativo e deve removê-lo do dispositivo.

  Recomendamos a renovação da licença antes da expiração para garantir proteção ininterrupta contra todas as ameaças de segurança.

Sobre a assinatura

Uma *assinatura do Kaspersky Endpoint Security* é um pedido de compra do aplicativo com parâmetros específicos (data de expiração, número de dispositivos protegidos). Você pode encomendar a assinatura do Kaspersky Endpoint Security junto de seu provedor de serviços (como, por exemplo, seu ISP). Você pode gerenciar sua assinatura na área de membros do site do provedor de serviços. Por exemplo, você pode renovar ou cancelar sua assinatura, reduzir o prazo da assinatura ou alterar o número de dispositivos protegidos por sua assinatura.

Uma assinatura pode ser limitada (por um ano, por exemplo) ou ilimitada (sem data de expiração). Para manter o Kaspersky Endpoint Security funcionando após o término do período de assinatura limitada, será necessário renová-la manualmente. Uma assinatura ilimitada será renovada automaticamente, desde que você tenha pagado o provedor de serviços previamente.

Se você usar o aplicativo com uma assinatura limitada, quando a assinatura expirar, você terá um período de carência para renová-la. O aplicativo permanecerá funcional durante o período de carência.

Após a expiração da assinatura de atualizações e o término do período de carência para a renovação da assinatura, o Kaspersky Endpoint Security continua funcionando, mas interrompe as atualizações dos bancos de dados do aplicativo.

Após a expiração da assinatura de atualizações e proteção e o término do período de carência para a renovação da assinatura, o Kaspersky Endpoint Security interrompe a proteção do computador.

Para usar o Kaspersky Endpoint Security com assinatura, você deve aplicar o código de ativação recebido pelo provedor de serviços. Quando você usa o aplicativo com uma assinatura, não pode usar um código de ativação diferente para renovar a sua assinatura. Você só poderá aplicar um código de ativação diferente depois que a assinatura expirar ou for cancelada. Para cancelar a assinatura, entre em contato com o provedor de serviços que vendeu o Kaspersky Endpoint Security para você.

Nota: será possível aplicar um código de ativação de assinatura diferente somente depois que a chave ativa for excluída. A assinatura não tem um arquivo de chave. Não é possível adicionar a assinatura como uma chave reserva. Uma chave reserva não pode ser adicionada quando a assinatura for usada.

Se você já estiver usando o Kaspersky Endpoint Security com uma licença válida, mas desejar usar o aplicativo com uma assinatura, remova a chave ativa atual para poder ativar o aplicativo usando uma chave de assinatura. O código de ativação anteriormente usado para ativar o aplicativo com este computador pode ser usado em um computador diferente.

Nota: as opções de assinatura possíveis podem variar dependendo do provedor de serviços. Além disso, alguns provedores de serviços podem optar por não oferecer um período de carência para renovar as assinaturas.

Sobre o certificado de licença

Um *certificado de licença* é um documento que você recebe junto com um arquivo de chave ou um código de ativação.

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

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

Sobre a chave

Uma *chave* é uma sequência de bits que você pode aplicar para ativar e então usar o aplicativo de acordo com os termos do Contrato de Licença de Usuário Final. As chaves são geradas por especialistas da Kaspersky.

Você pode adicionar uma chave ao aplicativo usando um dos seguintes métodos: aplicando um *arquivo de chave* ou inserindo um *código de ativação*. A chave é exibida na interface de aplicativo como uma sequência alfanumérica exclusiva depois que você a adiciona ao aplicativo.

A chave pode ser bloqueada pela Kaspersky se os termos do Contrato de Licença forem violados. Se a chave for bloqueada, você precisará adicionar outra se desejar usar o aplicativo.

Uma chave pode ser ativa ou de reserva.

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

Uma *chave reserva* é uma chave que dá ao usuário o direito de usar o aplicativo, mas que não está atualmente em uso. A chave reserva torna-se automaticamente ativa quando a licença associada à chave ativa atual expira. Uma chave reserva só pode ser adicionada se uma chave ativa já tiver sido adicionada.

Uma chave de licença de avaliação pode ser adicionada como chave ativa. Uma chave de licença de avaliação não pode ser adicionada como chave reserva. Uma chave reserva não pode ser adicionada quando a chave de licença de avaliação estiver ativa.

Sobre o código de ativação

Um *código de ativação* é uma sequência exclusiva de 20 letras e números. É necessário inserir um código de ativação para adicionar uma chave de licença para ativar o Kaspersky Endpoint Security. Você recebe o código de ativação no endereço de e-mail fornecido quando adquiriu o Kaspersky Endpoint Security ou quando solicitou a versão de avaliação do Kaspersky Endpoint Security.

Para ativar o aplicativo usando um código de ativação, é necessário acessar a Internet para se conectar aos servidores de ativação da Kaspersky.

Caso tenha perdido o código de ativação após instalar o aplicativo, entre em contato com o parceiro Kaspersky de quem adquiriu a licença.

Sobre o arquivo de chave

Um *arquivo de chave* é um arquivo com a extensão .key fornecido pela Kaspersky. Os arquivos de chave foram projetados para ativar o aplicativo adicionando uma chave de licença.

Você recebe um arquivo de chave no endereço de e-mail fornecido quando adquiriu o Kaspersky Endpoint Security ou quando solicitou a versão de avaliação do Kaspersky Endpoint Security.

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

Você pode restaurar um arquivo de chave se ele tiver sido excluído acidentalmente. Um arquivo de chave pode ser necessário para registrar uma Kaspersky CompanyAccount, por exemplo.

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

- Entre em contato com o vendedor da licença.
- Receba um arquivo de chave no site da Kaspersky usando o código de ativação disponível.

Sobre a coleta de dados

Contrato de Licença de Usuário Final

Ao ativar o Kaspersky Endpoint Security usando um código de ativação, você concorda em fornecer automaticamente as seguintes informações durante o uso do Kaspersky Endpoint Security para que seja possível verificar o uso legítimo do aplicativo e fornecer informações estatísticas sobre a distribuição e o uso dos produtos da Kaspersky:

- O tipo, a versão e a localização do Software instalado.
- As versões das atualizações instaladas.
- O identificador do computador e o identificador da instalação do Software no computador.
- O código de ativação e o identificador de ativação exclusivo da licença atual.
- O tipo, a versão e o tamanho da palavra do sistema operacional.
- O nome do ambiente virtual se o Software estiver instalado em um.
- Os identificadores dos componentes do Software ativos no momento do fornecimento das informações.
- A fonte de dados compatível.
- Tempo limite.

- Data e hora no computador do usuário.
- Versão do protocolo.
- Tipo de conteúdo do protocolo.
- Tamanho do conteúdo do protocolo.
- O tipo de compactação de dados usada.
- O tipo de assinatura no tíquete de ativação.
- Identificador do Centro de Ativação Regional.
- Hash do código de ativação calculado usando o algoritmo SHA1.
- Hash do corpo do tíquete calculado usando o algoritmo SHA1.
- Data e hora de criação do tíquete da licença.
- Identificador da ativação da licença.
- Identificador do tíquete da licença atual.
- Identificador de sequência de ticket da licença.
- Data e hora de ativação da licença.
- Data e hora de expiração da licença.
- Status da licença.
- Versão da licença.
- O identificador exclusivo do computador do usuário.
- Versão do cabeçalho do tíquete da licença.
- Nome do aplicativo.
- Tipo de dados transferidos.
- Versão do esquema de dados transferidos.
- A versão completa do sistema operacional.
- Descrição da máquina virtual usada.
- Lista de IDs para aplicativos compatíveis.

Ao usar os Servidores de atualização Kaspersky para baixar as atualizações, a fim de aumentar a eficiência do procedimento de atualização, você concorda em fornecer periodicamente as seguintes informações para a identificação do aplicativo durante as atualizações do banco de dados e do módulo:

- ID do software (AppID).
- ID da licença ativa.
- ID exclusivo da instalação do software (InstallationID).
- ID exclusivo da inicialização da tarefa de atualização (SessionID).
- Versão do aplicativo (BuildInfo).

Declaração da Kaspersky Security Network (KSN)

O uso da KSN pode aumentar a velocidade de reação do Software a ameaças de segurança de informações e da rede. Esse propósito é atingido ao:

- Determinar a reputação dos objetos verificados.
- Identificar novas ameaças (de difícil detecção) à segurança das informações, bem como as respectivas fontes.
- Tomar medidas imediatas para aumentar a proteção dos dados armazenados e processados por um usuário no computador.
- Reduzir a probabilidade de falsos positivos.
- Aumentar a eficiência dos componentes do aplicativo.
- Investigar uma infecção no computador de um usuário.
- Melhorar o desempenho dos produtos da Kaspersky.
- Receber informações de referência sobre a quantidade de objetos com reputação conhecida.
- Identificar e corrigir imediatamente erros relacionados à instalação, remoção e atualização do produto.

Ao utilizar a KSN, a Kaspersky receberá e processará automaticamente os dados. Os dados transmitidos pelo Usuário dependem do tipo de licença instalada e das configurações de uso da Kaspersky Security Network especificadas.

Se você usar uma licença para 1 a 4 nós, a Kaspersky receberá e processará automaticamente os dados a seguir durante o uso da Kaspersky Security Network:

- Informações sobre a licença usada: o tipo e o período de validade da licença, número de dias até a expiração da licença, identificador do parceiro de quem a licença foi adquirida, identificador do Centro de Ativação Regional, soma de verificação do código de ativação, hash do corpo do tíquete calculado usando o algoritmo SHA1, data e hora da criação do tíquete de licença, identificador de informações da licença, identificador do tíquete de licença, identificador da sequência do tíquete de licença, identificador exclusivo do computador do usuário, data a partir da qual o tíquete de licença começa a valer, data de expiração da validade do tíquete de licença, estado atual do tíquete de licença, versão do cabeçalho do tíquete, versão da licença, identificador do certificado de assinatura do cabeçalho do tíquete, soma de verificação do arquivo de chave, número de série do assinante do cabeçalho do tíquete, token de autenticação.

- Versão completa do software instalado; tipo do Software instalado; ID de atualização do Software; ID do serviço de reputação; ID do tipo de protocolo; ID de um centro de ativação regional; versão da lista de decisões revogadas do serviço de Software; ID do registro acionado nos bancos de dados de antivírus do Software; carimbo de data e hora do registro acionado nos bancos de dados de antivírus do Software; tipo do registro acionado nos bancos de dados de antivírus do Software; ID exclusiva da instância da instalação do aplicativo no computador; data de ativação da licença; data de expiração da licença; identificador da licença; status da licença usada pelo Software; tipo de soma de verificação do objeto que está sendo processado; nome do malware detectado ou do software legítimo que pode ser usado para causar danos ao dispositivo ou aos dados do usuário; soma de verificação do objeto que está sendo processado; soma de verificação do código de ativação do Software; versão completa do Software; ID exclusivo do dispositivo; ID do Software; soma de verificação do arquivo da chave do Software; ID do modelo de informações usado para fornecer a licença do Software; identificador do certificado usado para assinar o cabeçalho do tíquete de licença do Software; data e hora de criação do tíquete de licença do Software; a soma de verificação do tíquete de licença do Software; a versão do tíquete de licença do Software; a versão do código de ativação do Software; formato dos dados na solicitação para a infraestrutura do Titular dos Direitos; ID do tíquete de licença atual; o ID de componente do Software; o resultado da ação do Software; código de erro; endereço acessado do serviço Web (URL, IP); número da porta; endereço web da origem da solicitação de serviço da web (referenciador); chave pública do certificado; impressão digital do certificado digital do objeto verificado e algoritmo de hash.

Se você usar uma licença para 5 ou mais nós, a Kaspersky receberá e processará automaticamente os dados a seguir durante o uso da Kaspersky Security Network:

- Informações sobre a versão do sistema operacional (SO) e os service packs instalados no computador, a versão e as somas de verificação (MD5, SHA2-256, SHA1) do arquivo de kernel do SO, parâmetros do modo de execução do SO; versão do SO, número da compilação do SO, número da atualização do SO, edição do SO, informações estendidas sobre a edição do SO; versão do Service Pack do SO; data e hora da inicialização do SO; tempo de atraso do processamento do evento sobre a ação do SO no subsistema de análise comportamental; número de eventos da ação atrasada do SO do tipo atual; tempo de atraso de processamento do evento sobre a ação do SO no subsistema de defesa proativo; número de eventos processadas de ação do SO; número de eventos da ação processada síncrona do SO; atraso total de todos os eventos da ação do SO do tipo atual; tempo de atraso de processamento do evento sobre a ação do SO no subsistema de armazenamento de eventos persistentes; atraso total de todos os eventos da ação do SO; número de eventos da ação em espera síncrona do SO; data e hora do evento recebido de uma ação no SO.

- Informações sobre a última reinicialização do SO com falha: número de reinicializações com falha.

- Informações sobre o aplicativo instalado do Titular dos direitos e o status da proteção antivírus: ID de instalação do Software (PCID); Versão do registro do banco de dados do software; identificados exclusivo da instância da instalação do aplicativo no computador, tipo do aplicativo, ID do tipo do aplicativo, a versão completa do aplicativo instalado, a versão do identificador das configurações do aplicativo, o identificador do tipo de computador, o identificador exclusivo do computador em que o aplicativo está instalado, o identificador exclusivo do Usuário nos serviços do Titular de Direitos, idioma local e estado da operação, versão dos componentes do Software instalado e seus estados de operação, versão do protocolo usado para conectar com os serviços do Titular de Direitos; versão completa do software instalado; tipo do Software instalado; ID de atualização do Software; ID do serviço de reputação; ID do tipo de protocolo; ID de um centro de ativação regional; versão da lista de decisões revogadas do serviço de Software; ID do registro acionado nos bancos de dados de antivírus do Software; carimbo de data e hora do registro acionado nos bancos de dados de antivírus do Software; tipo do registro acionado nos bancos de dados de antivírus do Software; ID exclusiva da instância da instalação do aplicativo no computador; data de ativação da licença; data de expiração da licença; identificador da licença; status da licença usada pelo Software; tipo de soma de verificação do objeto que está sendo processado; nome do malware detectado ou do software legítimo que pode ser usado para causar danos ao dispositivo ou aos dados do usuário; soma de verificação do objeto que está sendo processado; soma de verificação do código de ativação do Software; versão completa do Software; ID do Software; soma de verificação do arquivo da chave do Software; ID do modelo de informações usado para fornecer a licença do Software; identificador do certificado usado para assinar o cabeçalho do tíquete de licença do Software; data e hora de criação do tíquete de licença do Software; a soma de verificação do tíquete de licença do Software; a versão do tíquete de licença do Software; a versão do código de ativação do Software; formato dos dados na solicitação para a infraestrutura do Titular dos Direitos; ID do tíquete de licença atual; o ID de componente do Software; o resultado da ação do Software; código de erro; endereço acessado do serviço Web (URL, IP); número da porta; endereço web da origem da solicitação de serviço da web (referenciador); número de ciclos atualização-aplicação para bases de dados antivírus; data e hora em que as bases de dados de antivírus foram atualizadas e aplicadas pela última vez; data e hora do lançamento nos bancos de dados do Software; versão do componente do Software; ID de atualização do Software; tipo do Software instalado; data e hora da inicialização do Inspetor do Sistema; data e hora da instalação do Software; probabilidade de enviar estatísticas pelo Inspetor do Sistema; código do evento que demorou mais tempo do que o tempo padrão a processar pelo Inspetor do Sistema; tempo de processamento da base de dados do evento que demorou mais tempo do que o tempo padrão a processar pelo Inspetor do Sistema; tempo máximo permitido para processamento de um evento pelo Inspetor do Sistema; tempo de processamento do evento que levou mais tempo do que o padrão para ser processado pelo Inspetor do Sistema; número total de eventos que demoraram mais tempo do que o tempo padrão para processar pelo Inspetor do Sistema.

- Informações sobre todos os objetos e operações processados: Veredito do software sobre o objeto sendo processado; código do diretório; tamanho do objeto que está sendo processado; soma de verificação (SHA256) do objeto que está sendo processado; número do software detectado no contexto do Inspetor do Sistema; data e hora da detecção do software pelo Inspetor do Sistema; detectar características; ID do registro acionado nos bancos de dados de antivírus do Software; motivo da detecção do software pelo Inspetor do Sistema; soma de verificação (MD5) do objeto que está sendo processado; resultado da verificação de integridade do módulo; nome do objeto que está sendo processado; tipo do registro acionado nos bancos de dados de antivírus do Software; caminho para o objeto que está sendo processado; o nome do objeto verificado; a data e hora da verificação; os endereços URL e de referência dos quais foi baixado; o tamanho dos arquivos verificados e os caminhos para eles; o sinal de arquivo; a data e hora da criação do arquivo; o nome, tamanho e somas de verificação (MD5, SHA2-256) do compactador (se o arquivo foi empacotado); a entropia do arquivo; o tipo de arquivo; o código do tipo de arquivo; o sinal, ID e formato do arquivo executável; a soma de verificação do objeto (MD5, SHA2-256); o tipo e o valor da soma de verificação suplementar do objeto; dados sobre a assinatura digital do objeto (certificado): dados sobre o editor do certificado, número de inicializações do objeto desde a última entrega de estatísticas, ID da tarefa de verificação do aplicativo, meio de recebimento de informações sobre a reputação do objeto, valor do filtro alvo, parâmetros técnicos das tecnologias de detecção aplicáveis; caminho para o objeto que está sendo processado; código do diretório.

- Para arquivos executáveis: a entropia das seções do arquivo, indicador de verificação de reputação ou indicador de assinatura de arquivo, nome, tipo, tipo de ID, soma de verificação (MD5) e o tamanho do aplicativo que foi carregado pelo objeto que está sendo validado, o caminho do aplicativo e os caminhos do modelo, um atributo indicando presença na lista de Autorun, data de entrada, lista de atributos, nome do compactador, informações sobre a assinatura digital do aplicativo: o certificado do editor, o nome do arquivo carregado no formato MIME, a data e hora de compilação do arquivo.

- Informações sobre aplicativos iniciados e os seus módulos: somas de verificação (MD5, SHA2-256) de arquivos em execução, tamanho, atributos, data de criação, nome do compactador (se o arquivo foi compactado), nomes de arquivos, informações sobre processos em execução no sistema (ID do processo (PID)), nome do processo, informações sobre a conta a partir da qual o processo foi iniciado, o aplicativo e o comando que iniciaram o processo, o caminho completo para os arquivos do processo e a linha de comando inicial, uma descrição do aplicativo ao qual o processo pertence (o nome do aplicativo e as informações sobre o editor, além dos certificados digitais usados e as informações necessárias para verificar a autenticidade ou as informações sobre a ausência de assinatura digital de um arquivo), e informações sobre os módulos carregados nos processos: seus nomes, tamanhos, tipos, datas de criação, atributos, somas de verificação (MD5, SHA2-256, SHA1), os caminhos para eles, informações do cabeçalho do arquivo PE, nomes dos compactadores (se o arquivo foi compactado), informações sobre a disponibilidade e validade dessas estatísticas, identificador do modo para gerar as estatísticas que estão sendo enviadas.

- Se forem detectadas ameaças ou vulnerabilidades, além das informações sobre o objeto detectado, são fornecidas informações sobre o identificador, a versão e o tipo do registro no banco de dados de antivírus, o nome da ameaça com base na classificação da Kaspersky, a data e hora da última atualização do banco de dados de antivírus, o nome do arquivo executável, a soma de verificação (MD5) do arquivo do aplicativo que solicitou o URL no qual a ameaça foi detectada, o endereço IP (IPv4 ou IPv6) da ameaça detectada, o identificador de vulnerabilidade e seu nível de ameaça, o URL e o referenciador da página da Web em que a vulnerabilidade foi detectada.

- Se um objeto potencialmente malicioso for detectado, são fornecidas informações sobre os dados na memória dos processos.

- Informações sobre ataque de rede: endereço IP do computador atacante e número da porta no computador do usuário visado pelo ataque de rede, ID do protocolo de ataque, nome e tipo de ataque.

- Informações sobre conexões de rede: versão e somas de verificação (MD5, SHA2-256, SHA1) do arquivo a partir do qual foi iniciado o processo que abriu a porta, caminho para o arquivo do processo e a respectiva assinatura digital, endereços IP local e remoto, número de portas de conexão locais e remotas, estado da conexão, carimbo de data e hora da abertura da porta.

- O URL e o endereço IP da página da Web onde o conteúdo danoso ou suspeito foi detectado, o nome, tamanho e soma de verificação do arquivo que solicitou o URL, o identificador, peso e grau da regra utilizada para obter um veredito, o objetivo do ataque.

- Informações sobre as atualizações do aplicativo instalado e bancos de dados de antivírus: status de conclusão da tarefa de atualização, tipo de erro que pode ter ocorrido durante o processo de atualização, o número de atualizações sem êxito, o identificador do componente do aplicativo que executa as atualizações.

- Informações sobre o uso da Kaspersky Security Network (KSN): identificador da KSN, identificador do aplicativo, versão completa do aplicativo, endereço IP despersonalizado do dispositivo do usuário, indicadores da qualidade do cumprimento das solicitações da KSN, indicadores da qualidade do processamento de pacotes da KSN, indicadores do número de solicitações da KSN e informações sobre os tipos de solicitações da KSN, data e hora do início do envio das estatísticas, data e hora do término do envio das estatísticas, informações sobre as atualizações de configuração da KSN: identificador da configuração ativa, identificador da configuração recebida, código de erro da atualização da configuração.

- Informações sobre eventos de log do sistema: hora do evento, nome do registro onde o evento foi detectado, tipo e categoria do evento, nome da fonte do evento e descrição do evento.

- Informações para determinar a reputação de arquivos e endereços URL: o endereço de URL no qual a reputação está sendo solicitada e o Referenciador, o tipo de protocolo da conexão, o identificador interno do tipo de aplicativo, o número da porta que está sendo utilizada, o identificador de Usuário, a soma de verificação do arquivo verificado (MD5), tipo de ameaça detectada, informações sobre o registro usado para detectar uma ameaça (identificador de registro para os bancos de dados de antivírus, o registro de data e hora e o tipo); chave pública do certificado; impressão digital do certificado digital do objeto verificado e algoritmo de hash.

- Dados sobre a distribuição territorial do aplicativo: data de instalação e ativação do aplicativo, ID do parceiro que fornece a licença para a ativação do aplicativo, ID do aplicativo, ID de localização do idioma do aplicativo, número de série da licença para a ativação do aplicativo, sinal de participação da KSN.

- Informações sobre a licença usada: o tipo e o período de validade da licença, número de dias até a expiração da licença, identificador do parceiro de quem a licença foi adquirida, identificador do Centro de Ativação Regional, soma de verificação do código de ativação, hash do corpo do tíquete calculado usando o algoritmo SHA1, data e hora da criação do tíquete de licença, identificador de informações da licença, identificador do tíquete de licença, identificador da sequência do tíquete de licença, identificador exclusivo do computador do usuário, data a partir da qual o tíquete de licença começa a valer, data de expiração da validade do tíquete de licença, estado atual do tíquete de licença, versão do cabeçalho do tíquete, versão da licença, identificador do certificado de assinatura do cabeçalho do tíquete, soma de verificação do arquivo de chave, número de série do assinante do cabeçalho do tíquete, token de autenticação.

- Informações sobre o hardware instalado no computador: tipo, nome, nome do modelo, versão do firmware, parâmetros de dispositivos integrados e conectados.

- Informações sobre o dispositivo: ID do dispositivo.

- Informações sobre a operação do componente Controle da Web: versão do componente, motivo da categorização, informações adicionais sobre o motivo da categorização, URL categorizado, endereço IP do host do objeto bloqueado/categorizado.

Além disso, para cumprir o objetivo declarado de aumentar a eficácia da proteção fornecida pelo aplicativo, a Kaspersky poderá receber objetos que podem ser explorados por invasores para danificar o computador e criar ameaças de segurança às informações. Esses objetos são:

- Arquivos executáveis ou não executáveis ou partes deles

- Áreas RAM do computador

- Setores envolvidos no processo de inicialização do SO

- Pacotes de dados do tráfego de rede

- Páginas da Web e e-mails que contenham objetos suspeitos e maliciosos

- Descrição de classes e instâncias de classes para o armazenamento de WMI

- Relatórios de atividade dos aplicativos

Os relatórios de atividade dos aplicativos contêm as seguintes informações sobre os arquivos e processos:

- Nome, tamanho e versão do arquivo sendo enviado, sua descrição e somas de verificação (MD5, SHA2-256, SHA1), ID do formato, nome do fabricante, nome do aplicativo ao qual o arquivo pertence, o caminho totalmente qualificado até o arquivo no computador e o código de modelo do caminho, data e hora da criação e atualização do arquivo.

- Data e hora inicial e final da validade do certificado, se o arquivo que está sendo enviado tem assinatura digital, data e hora em que o certificado foi assinado, nome do editor do certificado, informações sobre o titular do certificado, impressão e chave pública do certificado e algoritmos utilizados para calculá-los, número de série do certificado.
- Nome da conta que executou o processo.
- Checksums (MD5, SHA2-256, SHA1) para o nome do computador que está executando o processo.
- Cabeçalhos das janelas do processo.
- ID dos bancos de dados de antivírus, nome da ameaça identificada de acordo com a classificação da Kaspersky.
- Informações sobre a licença usada para o aplicativo, ID, tipo e data de expiração da licença.
- Horário local do computador no momento em que a informação foi fornecida.
- Os nomes e os caminhos dos arquivos que foram acessados pelo processo.
- URL - e endereços IP que foram acessados pelo processo.
- URL - e endereços IP dos quais o arquivo em execução foi baixado.

Além disso, para cumprir o objetivo declarado com relação à prevenção de falsos positivos, o Titular dos Direitos poderá receber arquivos executáveis e não executáveis confiáveis ou respectivas partes.

Ler a Declaração da Kaspersky Security Network

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Avançado**, clique em **Mostrar a Declaração da KSN**.

O Kaspersky Endpoint Security salva as seguintes informações em um arquivo de rastreamento:

- Informações sobre o dispositivo e o sistema operacional (ID exclusivo do dispositivo, tipo de dispositivo, endereços MAC dos dispositivos da rede, tipo de sistema operacional, versão do sistema operacional).
- Informações sobre a operação do aplicativo e os seus módulos.
- Informações sobre a assinatura (tipo de assinatura, região).
- Informações sobre a localidade de idioma, ID do aplicativo, personalização do aplicativo, versão do aplicativo, ID exclusivo de instalação do aplicativo, ID exclusivo do computador.
- Informações sobre o status da proteção antimalware do computador, bem como todos os objetos processados e detectados (nome do objeto detectado, data e a hora da detecção, endereço da Web a partir do qual ele foi baixado, nomes e tamanhos dos arquivos infectados e seus caminhos, endereço IP do computador que realizou o ataque e o número da porta do computador que era o alvo do ataque de rede, lista de atividades de malware e endereços da Web indesejados) e as decisões pertinentes tomadas pelo aplicativo e pelo usuário.
- Informações sobre aplicativos baixados pelo usuário (endereço da Web, atributos, tamanho do arquivo e informações sobre o processo que baixou o arquivo).

- Informações sobre os aplicativos iniciados e seus módulos (tamanho, atributos, data de criação, detalhes de cabeçalho PE, região, nome, local e empacotadores).
- Informações sobre erros e uso da interface do aplicativo da Kaspersky instalado.
- Informações sobre conexões de rede: endereço IP do computador remoto e do computador do usuário, números das portas através das quais a conexão foi estabelecida e o protocolo de rede da conexão.
- Informações sobre os pacotes de rede recebidos e enviados pelo computador pelas redes de TI e de telecomunicações.
- Informações sobre mensagens instantâneas e e-mails enviados e recebidos.
- Informações sobre endereços Web visitados: a hora em que a conexão foi estabelecida usando um protocolo aberto, dados de login e senha do site e o conteúdo dos cookies.
- Certificado público do servidor.

Os arquivos de rastreamento contêm apenas as informações necessárias para corrigir defeitos no aplicativo. A Kaspersky utiliza arquivos de rastreamento para investigar incidentes associados a erros na operação do aplicativo Kaspersky Endpoint Security.

Por padrão, a criação de arquivos de rastreamento é desativada. Você pode ativar a geração de arquivos de rastreamento nos ajustes do aplicativo.

Os arquivos de rastreamento só podem ser enviados manualmente à Kaspersky. O aplicativo não envia os arquivos de rastreamento à Kaspersky automaticamente.

É possível escolher como os arquivos de rastreamento são enviados à Kaspersky.

Antes de enviar arquivos de rastreamento à Kaspersky, revise os dados que eles contêm.

Importante: os arquivos de rastreamento podem conter informações pessoais ou sigilosas. Ao enviar arquivos de rastreamento à Kaspersky, você aceita fornecer todos os dados contidos neles e concorda com o método usado para enviá-los.

Os arquivos (ou suas partes) que podem ser explorados por intrusos para danificar o computador ou os dados também podem ser enviados à Kaspersky para análise adicional.

A Kaspersky protege quaisquer informações recebidas de acordo com a lei e as regras da Kaspersky aplicáveis. Os dados são transmitidos por meio de um canal seguro.

A participação no Kaspersky Security Network é voluntária. A decisão de participar ou não é tomada quando você instala o aplicativo. De qualquer forma, você pode mudar sua decisão posteriormente, a qualquer momento.

Ativar o Kaspersky Endpoint Security

Importante: antes de ativar o Kaspersky Endpoint Security, verifique se a data e a hora configuradas no computador coincidem com a data e a hora atuais.

Ativar o aplicativo envolve adicionar uma chave ao aplicativo.

Nota: é necessário estar conectado à Internet para ativar o aplicativo.

Ativar a versão de avaliação

1. Abra a janela principal do aplicativo.
2. Na barra lateral da janela principal do aplicativo, clique em **Licença**.

   A janela **Licença** será exibida.
3. Na janela **Licença**, clique em **Ativar**.

   O Kaspersky Endpoint Security se conecta aos servidores de ativação da Kaspersky e envia os dados para verificação. Se a verificação for bem-sucedida, o aplicativo receberá e adicionará a chave da versão de avaliação gratuita.

   Importante: uma versão de avaliação do Kaspersky Endpoint Security somente poderá ser ativada se o aplicativo ainda não tiver sido ativado no computador.

Ativar o aplicativo com um código de ativação

1. Abra a janela principal do aplicativo.
2. Na barra lateral da janela principal do aplicativo, clique em **Licença**.

   A janela **Licença** será exibida.
3. Na janela **Licença**, digite o código de ativação que recebeu ao comprar o Kaspersky Endpoint Security.
4. Clique em **Ativar**.

   Nota: o código de ativação é uma combinação exclusiva de vinte letras latinas e números no formato xxxxx-xxxxx-xxxxx xxxxx.

   O aplicativo se conecta aos servidores de ativação da Kaspersky e envia o código de ativação para verificar sua autenticidade. Se o código de ativação for verificado com êxito, o aplicativo receberá e adicionará automaticamente a chave de licença.

   Nota: dependendo do código de ativação que você recebeu, talvez seja necessário preencher um formulário de registro.

   Se a verificação do código falhar, será exibida uma notificação correspondente. Nesse caso, entre em contato com o fornecedor de software que forneceu esse código de ativação.

Depois de ativar o aplicativo com o código de ativação, será possível ver as seguintes informações na janela **Licença**:

- Status da licença ou assinatura
- Chaves ativas

- Chaves reservas (caso existam)
- O tipo de licença e o número de computadores nos quais é possível usar o aplicativo com a licença ou assinatura atual
- Recursos do aplicativo que estão disponíveis na licença ou assinatura atual
- Data e hora de expiração da licença
- Número de dias até a licença expirar

Exibir informações da licença

Exibir informações da licença

1. Abra a janela principal do aplicativo.
2. Na barra lateral da janela principal do aplicativo, clique em **Licença**.

   A janela **Licença** será exibida.

A janela **Licença** pode conter as seguintes informações:

- Status da licença ou assinatura
- Chaves ativas
- Chaves reservas (caso existam)
- O tipo de licença e o número de computadores nos quais é possível usar o aplicativo com a licença ou assinatura atual
- Recursos do aplicativo que estão disponíveis na licença ou assinatura atual
- Data e hora de expiração da licença
- Número de dias até a licença expirar

Gerenciar licenças e assinaturas

Você precisará renovar a licença se a licença associada à chave ativa tiver expirado e nenhuma chave reserva tiver sido adicionada. Quando a licença expirar, o aplicativo continua funcionando com recursos limitados (atualizações, Kaspersky Security Network, Controle da Web e Criptografia de disco do FileVault via Kaspersky Security Center ficam indisponíveis). É possível continuar usando todos os componentes do aplicativo e executar as verificações de malware, mas somente com os bancos de dados de antimalware instalados antes da expiração da licença.

Importante: quando os bancos de dados antimalware estão desatualizados, o computador corre um risco maior de infecção.

Renovar uma licença

1. Na barra lateral da janela principal do aplicativo, clique em **Centro de Proteção**.

   A janela **Centro de Proteção** é aberta.

2. Na janela **Centro de Proteção**, clique em **Renovar**.

   Será exibida uma página da Web com informações sobre a renovação da licença por meio da loja on-line ou dos parceiros da Kaspersky. Quando você renova uma licença pela loja virtual, um código de ativação do Kaspersky Endpoint Security é enviado para o endereço de e-mail informado no formulário de pedido depois que o pagamento é efetuado.

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 sob uma assinatura ilimitada, o Kaspersky Endpoint Security renova a sua assinatura sem que você precise executar qualquer ação.

Se você usar o aplicativo com uma assinatura limitada e o período de carência para renovar a assinatura terminar, o Kaspersky Endpoint Security notificará você e interromperá as tentativas de renovar automaticamente a assinatura e atualizar os bancos de dados do aplicativo.

Você pode renovar sua assinatura manualmente entrando em contato com o fornecedor que lhe vendeu o Kaspersky Endpoint Security.

Renovar sua assinatura

1. Abra a janela principal do aplicativo.

2. Na barra lateral da janela principal do aplicativo, clique em **Licença**.

   A janela **Licença** será exibida.

3. Na janela **Licença**, clique em **Visitar site do provedor de serviços**.

   O site do seu provedor de serviços é aberto.

O status da assinatura pode ficar desatualizado. Nesse caso, você deve atualizar o status da assinatura manualmente. Se você não tiver uma assinatura atual, o Kaspersky Endpoint Security interromperá a atualização dos bancos de dados do aplicativo (se você tiver uma assinatura de atualizações) ou deixará de proteger o computador (se você tiver uma assinatura de atualizações e proteção).

Atualizar status da assinatura

1. Abra a janela principal do aplicativo.

2. Na barra lateral da janela principal do aplicativo, clique em **Licença**.

   A janela **Licença** será exibida.

3. Na janela **Licença**, clique no botão ↻.

Comparação da funcionalidade do aplicativo para estações de trabalho conforme o tipo de licença

O conjunto de funcionalidades do Kaspersky Endpoint Security disponível nas estações de trabalho depende do tipo de licença (consulte a tabela abaixo).

Comparação de recursos do Kaspersky Endpoint Security

Recurso	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
Proteção Avançada Contra Ameaças						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Detecção de Comportamento	✓	✓	✓	✓	✓	✓
Prevenção de Exploits	✓	✓	✓	✓	✓	✓
Mecanismo de Remediação	✓	✓	✓	✓	✓	✓
Proteção Essencial Contra Ameaças						
Proteção Contra Ameaças ao Arquivo	✓	✓	✓	✓	✓	✓
Proteção Contra Ameaças da Web	✓	✓	✓	✓	✓	✓
Proteção Contra Ameaças ao Correio	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓
Proteção Contra Ameaças à Rede	✓	✓	✓	✓	✓	✓
Controles de Segurança						
Controle de Dispositivos	✓	✓	✓	✓	✓	✓
Controle da Web	✓	✓	✓	✓	✓	✓
Criptografia de Dados						
Criptografia de disco FileVault	–	✓	✓	✓	✓	✓
Detection and Response						
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓
Kaspersky Sandbox *(A licença do Kaspersky Sandbox deve ser adquirida separadamente)*	✓	✓	✓	✓	✓	✓

Executar tarefas comuns

Abrir e sair do aplicativo

Após a conclusão da instalação, o aplicativo será automaticamente iniciado e o ícone do aplicativo aparecerá na barra de menus.

Abra o aplicativo

Na barra de menus, clique no ícone do aplicativo e escolha **Kaspersky Endpoint Security**.

Encerrar o aplicativo

Na barra de menus, clique no ícone do aplicativo e escolha **Sair**.

Quando você sai do aplicativo, o processo do aplicativo é removido da memória do computador.

Importante: depois de sair do aplicativo Kaspersky Endpoint Security, o computador não estará mais protegido e poderá ser infectado, provocando risco de perda de dados.

Exibir o status de proteção do computador

O indicador de status da proteção informa sobre problemas de proteção do computador. Este indicador tem a forma de um escudo e está localizado na janela principal do aplicativo. Dependendo do status da proteção do computador, a cor do indicador pode mudar. Caso o Kaspersky Endpoint Security detecte alguma ameaça de segurança, uma mensagem sobre as ameaças aparecerá na janela principal do aplicativo e a cor do indicador mudará.

A cor do indicador pode mudar das seguintes maneiras:

- **Verde**. O seu computador está apropriadamente protegido.

  Um indicador verde significa que os bancos de dados antimalware estão atualizados e que todos os componentes do aplicativo foram configurados como recomendando pela Kaspersky. Nenhum objeto malicioso foi detectado ou os objetos maliciosos detectados foram neutralizados.

- **Amarelo**. O nível de proteção do computador está reduzido.

  Um indicador amarelo significa que o Kaspersky Endpoint Security conhece um problema. Esses problemas incluem pequenos desvios das configurações de proteção recomendadas ou bancos de dados do aplicativo ligeiramente desatualizados.

- **Vermelho**. O computador tem risco de infecção.

  Um indicador vermelho significa que existem problemas perigosos que podem levar à infecção do computador e à perda de dados. Por exemplo, os bancos de dados do aplicativo antimalware estão muito desatualizados, o aplicativo não está ativado ou objetos maliciosos foram detectados.

  Recomendamos que você corrija quaisquer problemas e lide com as ameaças à segurança o mais rápido possível.

Exibição do status operacional dos componentes instalados

O Kaspersky Endpoint Security permite verificar o status dos componentes do aplicativo instalados na janela **Segurança**. O indicador ao lado do nome de cada componente reflete seu status.

Exibição do status do componente

1. Abra a janela principal do aplicativo.
2. Na barra lateral da janela principal do aplicativo, clique em **Segurança**.

   A janela **Segurança** é aberta.

Os seguintes indicadores de status podem ser exibidos:

	O componente está em execução.
	O componente está sendo executado e gerenciado por uma política de segurança.
	O componente apresentou defeito.
	O componente apresentou defeito e é gerenciado por uma política de segurança.
	O componente está desligado.
	O componente é desativado e gerenciado por uma política de segurança.
	O componente está pausado.
	O componente não é compatível com a licença atual.

Nota: Para alguns componentes, também é possível usar o menu de 3 pontos ao lado do nome do componente para abrir um relatório ou definir as configurações do componente.

Desativar e retomar a proteção do computador

Por padrão, o Kaspersky Endpoint Security é iniciado após a inicialização do sistema operacional e protege o computador até que ele seja desligado. Todos os componentes de proteção (Proteção Contra Ameaças ao Arquivo, Proteção Contra Ameaças da Web e Proteção Contra Ameaças à Rede) estão ativados e em execução.

Você pode desativar a proteção completamente ou desativar componentes de proteção específicos.

Importante: a Kaspersky recomenda que você não desative a proteção ou os componentes de proteção, pois isso poderá resultar na infecção do computador e na perda de dados.

Quando a proteção do computador for desativada:

- O ícone do aplicativo na barra de menus está inativo.
- O indicador do status da proteção na janela principal do aplicativo está em vermelho.

Quando um ou mais componentes de proteção estão desativados, o indicador do status da proteção fica vermelho ou amarelo.

Nota: desativar ou pausar os componentes de proteção não afeta as tarefas de verificação nem a tarefa de atualização.

É possível desativar/retomar a proteção do computador de uma das seguintes maneiras:

- Pelo ícone do aplicativo
- Na janela de ajustes do aplicativo
- No menu **Proteção**

Desativar/retomar a proteção do computador pelo ícone do aplicativo

1. Na barra de menus, clique no ícone do aplicativo e escolha **Desativar a proteção**/**Ativar a proteção**.

   Quando você desliga a proteção, uma solicitação de credenciais do administrador é exibida.

2. Quando as credenciais de administrador forem solicitadas, insira um nome e uma senha de administrador e confirme que você deseja desativar a proteção.

Desativar/reiniciar a proteção do computador na janela de ajustes do aplicativo

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Geral**, desmarque/marque a caixa de seleção **Ativar proteção**.

Desativar/retomar a proteção do computador a partir da barra de menus

Na barra de menus, clique em **Proteção** > **Desativar a proteção**/**Ativar a proteção**.

Importante: caso você tenha desativado a proteção do computador, ela não será automaticamente reativada quando o Kaspersky Endpoint Security for reiniciado. Você precisará reativar manualmente o componente de proteção.

Desativar um componente de proteção

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **<nome do componente>**, desmarque a caixa de seleção **Ativar <nome do componente>**.

Importante: se você desativar um componente de proteção, ele não será automaticamente reativado quando o Kaspersky Endpoint Security for reiniciado. Você precisará reativar manualmente o componente de proteção.

Ativar um componente de proteção

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **<nome do componente>**, selecione a caixa de seleção **Ativar <nome do componente>**.

Para ativar a proteção do computador ou componentes de proteção, você também pode usar o Centro de Proteção. Desativar a proteção do computador ou os componentes de proteção aumenta consideravelmente o risco de infecção do seu computador. É por isso que o Centro de Proteção lhe informa quando a proteção do computador estiver desativada.

Usar o Centro de Proteção

O *Centro de Proteção* é um recurso do Kaspersky Endpoint Security que ajuda a analisar e resolver problemas e ameaças à segurança do computador.

Abrir o Centro de Proteção

Na barra lateral da janela principal do aplicativo, clique em **Centro de Proteção**.

No Centro de Proteção, você encontra informações sobre ameaças ativas, exibe o estado dos bancos de dados do aplicativo e descobre se a proteção de algum componente está desativada.

Nota: se o administrador do sistema da organização permitir que o Controle da Web bloqueie o acesso a recursos perigosos da Web, o Kaspersky Endpoint Security exibe a notificação **O Controle da Web está ativado** no Centro de Proteção.

Para cada problema ou ameaça, o Kaspersky Endpoint Security sugere ações que você pode executar para resolver o problema ou a ameaça. Por exemplo, se o Kaspersky Endpoint Security detectar arquivos infectados no computador, você poderá clicar em **Desinfectar**. Se os bancos de dados antimalware estiverem desatualizados, será possível clicar em **Atualizar**. Você pode corrigir um problema ou neutralizar uma ameaça imediatamente ou mais tarde.

Para corrigir um problema ou neutralizar uma ameaça imediatamente

Clique no botão com o nome da ação recomendada para corrigir o problema ou neutralizar a ameaça.

O aplicativo executa a ação selecionada.

Se você fechar o Centro de Proteção sem neutralizar as ameaças perigosas, o indicador de status da proteção na janela principal do aplicativo continuará em vermelho para alertá-lo sobre essas ameaças.

Executar tarefas de verificação

A tarefa de Verificação Completa padrão está incluída no Kaspersky Endpoint Security. Durante a execução dessa tarefa, o aplicativo verifica a memória, os objetos de inicialização e todas as unidades internas do computador em busca de vírus e outros malwares.

Executar uma verificação completa do computador

1. Na barra lateral da janela principal do aplicativo, clique em **Verificação**.

   Será exibida a janela **Verificação**.

2. Clique no botão **Verificação completa**.

Uma verificação completa do computador é iniciada.

A tarefa de Verificação Rápida padrão está incluída no Kaspersky Endpoint Security. Durante a execução dessa tarefa, o aplicativo verifica as áreas mais importantes do computador (memória, objetos de inicialização e pastas do sistema) em busca de vírus e outros malwares.

Executar uma verificação rápida do computador

1. Na barra lateral da janela principal do aplicativo, clique em **Verificação**.

   Será exibida a janela **Verificação**.

2. Clique no botão **Verificação rápida**.

Uma verificação rápida do computador é iniciada.

Se você deseja verificar um objeto específico em busca de vírus e outros tipos de malware, como um disco interno, uma pasta, um arquivo ou um disco removível, é possível executar a tarefa de Verificação Personalizada.

Verificar um item selecionado

Siga um destes procedimentos:

- Clique com o botão direito em um item selecionado e escolha **Verificar malwares**.
- Arraste um item selecionado para o ícone do aplicativo no Dock.
- Arraste um item selecionado para a janela **Verificação**.

Você pode ver os resultados das tarefa de verificação concluídas na janela **Relatórios**.

Nota: o Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.

Configurar o início automático de uma tarefa de verificação agendada

Você pode criar uma programação para iniciar as tarefas de Verificação Rápida e Verificação Completa. O Kaspersky Endpoint Security verifica automaticamente todo o computador ou áreas específicas do computador, de acordo com a programação configurada.

Programar uma tarefa de verificação na janela Verificação

1. Na barra lateral da janela principal do aplicativo, clique em **Verificação**.

   Será exibida a janela **Verificação**.

2. Clique em **Agendar a verificação**.

   Uma caixa de diálogo é aberta onde você poderá definir o agendamento.

3. Selecione a caixa de seleção **Verificação completa** ou **Verificação rápida**.

4. Especifique a frequência de verificação e o horário do início da verificação.

5. Clique em **OK**.

Programar uma tarefa de verificação na janela Configurações

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Verificação**, clique em **Agendamento**.

3. Na janela que se abre, marque a caixa de seleção ao lado do nome da tarefa de verificação que você deseja iniciar em uma programação.

4. Configure a frequência e a hora da tarefa de verificação.

5. Clique em **OK** para salvar as alterações feitas no agendamento da tarefa de verificação.

Você pode visualizar os resultados da tarefa de verificação na janela **Relatórios**.

Atualizar os bancos de dados do aplicativo

Os servidores de atualização Kaspersky dedicados são a principal fonte de atualização do Kaspersky Endpoint Security. O Kaspersky Endpoint Security também pode usar pontos de distribuição, pastas locais ou outros servidores da Web como *fonte de atualização*.

Nota: é necessária uma conexão com a Internet para baixar as atualizações dos servidores de atualização.

Por padrão, o Kaspersky Endpoint Security verifica periodicamente se há atualizações nos servidores de atualização Kaspersky. Se novas atualizações estiverem disponíveis em um servidor, o Kaspersky Endpoint Security faz o download em segundo plano e as instala no seu computador.

Iniciar uma atualização do Kaspersky Endpoint Security

1. Na barra lateral da janela principal do aplicativo, clique em **Atualização**.

   Será exibida a janela **Atualização**.

2. Clique em **Atualizar**.

   O aplicativo verifica se há atualizações. Se houver qualquer atualização disponível, o aplicativo irá baixar e instalar tal atualização no seu computador.

Também é possível iniciar uma tarefa de atualização de uma das seguintes maneiras:

- Clique no ícone do aplicativo e escolha **Atualização**.
- Na barra de menus, selecione Proteção > **Atualização**.

Você pode modificar o modo que o Kaspersky Endpoint Security atualiza os bancos de dados do aplicativo. Por padrão, o aplicativo atualiza os bancos de dados automaticamente.

Ativar/desativar downloads automáticos de atualizações dos bancos de dados do Kaspersky Endpoint Security

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Atualização**, na seção **Bancos de dados**, marque/desmarque a caixa de seleção **Baixar atualizações automaticamente**.

Você pode ver os resultados das tarefas de atualização concluídas na janela **Relatórios**.

Observação: A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinaturas de antimalware e atualizações de base de código), bem como a funcionalidade KSN, podem não estar disponíveis no software nos EUA.

O que fazer se o acesso ao arquivo estiver bloqueado

O aplicativo Kaspersky Endpoint Security bloqueia o acesso a arquivos e aplicativos infectados. Se um arquivo estiver infectado, ele precisará ser desinfectado para que você possa acessá-lo.

Desinfectar um objeto detectado

1. Na barra de menus, selecione **Proteção** > **Objetos detectados**.

   Será exibida a janela **Objetos detectados**.

2. Na seção **Objetos detectados**, clique em ⋯, próximo ao arquivo desejado, e selecione **Desinfectar**.

   O aplicativo inicia a desinfecção do objeto selecionado. Durante a desinfecção do objeto, o aplicativo exibirá uma caixa de diálogo na qual você poderá escolher a ação que será executada no objeto.

Desinfetar todos os objetos detectados

1. Na barra de menus, selecione **Proteção** > **Objetos detectados**.

   Será exibida a janela **Objetos detectados**.

2. Na seção Objetos detectados, clique em **Desinfectar tudo**.

   O aplicativo inicia a desinfecção de objetos detectados. Durante a desinfecção do objeto, o aplicativo exibirá uma caixa de diálogo na qual você poderá escolher a ação que será executada no objeto. Se você marcar a caixa de seleção **Aplicar a todos** na janela de notificação após escolher uma ação, o aplicativo executará a mesma ação em todos os arquivos desse tipo.

Se tiver certeza de que os arquivos sendo bloqueados pela Proteção Contra Ameaças ao Arquivo são seguros, poderá incluí-los na Zona Confiável.

Restaurar um arquivo que foi excluído ou desinfectado pelo aplicativo

Às vezes, não é possível salvar arquivos totalmente durante o processo de desinfecção. Se um arquivo desinfectado continha informação importante que fica parcialmente ou completamente inacessível após a desinfecção, você pode tentar restaurar o arquivo original da cópia de segurança.

Restaurar um arquivo que foi excluído ou modificado pelo aplicativo durante a desinfecção

1. Na barra de menus, selecione **Proteção** > **Objetos detectados**.

   Será exibida a janela **Objetos detectados**.

2. Na seção **Efetuar backup**, clique em ⋯ próximo ao arquivo que você deseja restaurar.

   O menu suspenso é aberto.

3. Selecione **Restaurar o arquivo**.

   Uma janela para especificar o nome do arquivo, a tag e a pasta na qual o arquivo será restaurado é aberta. Por padrão, o nome e o local do arquivo original já estão especificados.

4. Especifique o nome do arquivo e a pasta na qual ele será restaurado.

5. Clique em **Salvar**.

O aplicativo restaura o arquivo no local especificado com o nome especificado.

É necessário verificar o arquivo quanto à presença de malware imediatamente após restaurá-lo. É possível que o objeto possa ser desinfectado usando bancos de dados atualizados sem ser corrompido.

Importante: recomendamos que você não restaure cópias de segurança de arquivos a menos que a restauração seja absolutamente necessária, pois isso pode levar à infecção do computador.

Exibir o relatório de funcionamento do aplicativo

É possível visualizar um relatório do Kaspersky Endpoint Security que lista todos os objetos detectados na guia **Objetos processados**. Os eventos do sistema são exibidos na guia **Eventos do sistema**. Além disso, um relatório detalhado e separado é criado para cada um dos seguintes componentes de aplicativo: Proteção Contra Ameaças ao Arquivo, Proteção Contra Ameaças da Web, Proteção Contra Ameaças à Rede, Detecção de Comportamento e as tarefas de verificação e atualização.

Abrir a janela Relatórios

Na barra de menus, selecione **Proteção** > **Relatórios**.

O que fazer se forem exibidas janelas de notificação

As notificações do aplicativo, que aparecem na forma de janelas de notificações, informam sobre eventos do aplicativo que exigem a sua atenção.

Se uma notificação for exibida na tela, selecione uma das opções sugeridas. A melhor opção é aquela definida como padrão pelos especialistas da Kaspersky.

Configuração avançada do aplicativo

Escopo da proteção do computador

Os objetos detectados pelo Kaspersky Endpoint Security são divididos em categorias de acordo com diversos atributos. O aplicativo pesquisa sempre a existência de vírus, worms, Cavalos de Troia e ferramentas maliciosas. Estes programas podem provocar danos importantes no computador. Para assegurar a proteção mais confiável do seu computador, você pode estender a lista de objetos detectáveis ativando o aplicativo para verificar o software legítimo que pode ser usado por intrusos para danificar o seu computador ou os seus dados pessoais.

Os objetos abrangidos pela proteção do Kaspersky Endpoint Security são agrupados da seguinte maneira:

- **Vírus, worms, trojans, ferramentas maliciosas, adwares e discadores automáticos**.

  Esta categoria inclui:

  - Todos os tipos de malware.
  - Software que pode ser inconveniente ao exibir anúncios (como banners) no seu computador ou que substituem os resultados de pesquisa no seu navegador por sites de publicidade.
  - Aplicativos que secretamente estabelecem conexões telefônicas através do modem de um computador.

  A proteção contra todos os tipos de malware corresponde ao nível de segurança mínimo necessário. De acordo com as recomendações dos especialistas da Kaspersky, o Kaspersky Endpoint Security sempre monitora objetos que pertencem a essa categoria.

- **Softwares legítimos que podem ser usados por intrusos para danificar seu computador ou dados pessoais**. Esta categoria inclui o software legítimo que pode ser usado por intrusos para danificar o seu computador ou os seus dados pessoais, tal como aplicativos de administração remota.

Selecionar as categorias de objetos a detectar

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Ameaças**, na seção **Objetos a detectar**, marque as caixas de seleção ao lado das categorias de objetos a serem detectadas.

   Nota: o Kaspersky Endpoint Security sempre protege o seu computador contra vírus, worms, Cavalos de Troia, ferramentas maliciosas, adware e discadores automáticos. Por esse motivo, não é possível desmarcar a caixa de seleção dessa categoria.

Dependendo das categorias selecionadas de objetos a detectar, o Kaspersky Endpoint Security usa alguns ou todos seus bancos de dados antimalware ao executar a Proteção Contra Ameaças ao Arquivo, a Proteção Contra Ameaças da Web e as tarefas de verificação.

Nota: se o Kaspersky Endpoint Security classificar um aplicativo como malware, mas você acredita que ele é seguro, poderá adicionar este aplicativo à Zona Confiável.

A *Zona Confiável* é uma lista de objetos que o Kaspersky Endpoint Security não verifica ou monitora. Por exemplo, poderá ser necessário adicionar objetos à Zona Confiável se o Kaspersky Endpoint Security bloquear o acesso a um arquivo, aplicativo ou site, mesmo se você tiver certeza de que o objeto, aplicativo ou endereço da Web é inofensivo.

Quando um aplicativo é adicionado à Zona Confiável, suas atividades de arquivos e de rede (incluindo as atividades suspeitas) não são mais monitoradas. Contudo, o Kaspersky Endpoint Security continua verificando o arquivo executável e o processo do aplicativo confiável.

Nota: Quando um administrador configura a política para proibir a edição da zona confiável, os usuários não podem acessar os ajustes dela.

Adicionar/remover um arquivo ou uma pasta da lista de arquivos e pastas confiáveis

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.
   É aberta a janela de ajustes do aplicativo.
2. Na guia **Ameaças**, na seção **Exclusões**, clique em **Zona Confiável**.
   Será exibida a janela de configurações da Zona Confiável.
3. Na guia **Arquivos e pastas**, edite a lista de arquivos e pastas confiáveis:
   - Para adicionar um arquivo ou uma pasta à lista:
     a. Clique em +.
        Será exibida uma caixa de diálogo na qual você poderá selecionar um arquivo ou uma pasta.
     b. Selecione o arquivo ou a pasta que deseja adicionar.
     c. Clique em **Abrir**.
   - Para remover um arquivo ou uma pasta da lista:
     a. Selecione o arquivo ou a pasta que deseja remover da lista de arquivos e pastas confiáveis.
     b. Clique em –.
4. Clique em **OK**.

Adicionar/remover um endereço da Web confiável da lista de endereços da Web confiáveis

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.
   É aberta a janela de ajustes do aplicativo.
2. Na guia **Ameaças**, na seção **Exclusões**, clique em **Zona Confiável**.
   Será exibida a janela de configurações da Zona Confiável.
   Você também pode abrir esta janela clicando no botão **Zona Confiável** na seção **Geral** da guia **Essencial**.

3. Na guia **Endereços da Web**, edite a lista de Endereços da Web confiáveis:

   - Para adicionar um endereço da Web à lista:

     a. Clique em +.

     b. Insira o endereço da Web que deseja adicionar à lista.

     c. Clique em **OK**.

   - Para remover um endereço da Web da lista:

     a. Selecione um endereço da Web que você deseja remover.

     b. Clique em –.

4. Clique em **OK**.

Por padrão, a lista de endereços da Web confiáveis está vazia.

Adicionar/remover um aplicativo confiável da lista de aplicativos confiáveis

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.
   É aberta a janela de ajustes do aplicativo.

2. Na guia **Ameaças**, na seção **Exclusões**, clique em **Zona Confiável**.
   Será exibida a janela de configurações da Zona Confiável.
   Você também pode abrir esta janela clicando no botão **Zona Confiável** na seção **Geral** da guia **Essencial**.

3. Na guia **Aplicativos confiáveis**, edite a lista de aplicativos confiáveis:

   - Para adicionar um aplicativo à lista:

     a. Clique em +.
     Abre uma janela onde você pode especificar os parâmetros do aplicativo necessário.

     b. Especifique os seguintes parâmetros do aplicativo que deseja adicionar:

     - **Caminho**
     - **Requisito de assinatura de código**

     > **Nota:** Você pode inserir os valores desses dois parâmetros manualmente ou clicar no botão **Selecionar** e selecionar o aplicativo que deseja adicionar na janela exibida. Nesse caso, os valores desses parâmetros serão inseridos automaticamente.

c. Na seção **Opções**, selecione pelo menos um tipo de atividade que você não deseja que seja monitorada pelo aplicativo Kaspersky Endpoint Security:

- **Não monitorar a atividade de arquivos**
- **Não monitorar a atividade de rede**

d. Clique em **OK**.

- Para remover um aplicativo da lista:

a. Selecione um aplicativo que deseja remover.

b. Clique em –.

Por padrão, a lista de aplicativos confiáveis está vazia.

Editar um aplicativo confiável

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.
   É aberta a janela de ajustes do aplicativo.
2. Na guia **Ameaças**, na seção **Exclusões**, clique em **Zona Confiável**.
   Será exibida a janela de configurações da Zona Confiável.
   Você também pode abrir esta janela clicando no botão **Zona Confiável** na seção **Geral** da guia **Essencial**.
3. Na guia **Aplicativos confiáveis**, selecione um aplicativo que deseja editar.
4. Clique em **Editar**.
5. Na janela exibida, edite os parâmetros do aplicativo.
6. Clique em **OK**.

Ativar o monitoramento de um endereço da Web confiável

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.
   É aberta a janela de ajustes do aplicativo.
2. Na guia **Ameaças**, na seção **Exclusões**, clique em **Zona Confiável**.
   Será exibida a janela de configurações da Zona Confiável.
3. Na guia **Endereços da Web**, desmarque a caixa de seleção ao lado do endereço da Web que deseja que o aplicativo Kaspersky Endpoint Security monitore.
4. Clique em **OK**.

Proteção Contra Ameaças ao Arquivo

A Proteção Contra Ameaças ao Arquivo evita a infecção do sistema de arquivos do computador. O componente é iniciado durante a inicialização do sistema operacional, permanece na memória do computador e verifica todos os arquivos abertos, salvos ou executados no computador e em todas as unidades conectadas em busca de malware. Se você desativar a Proteção Contra Ameaças ao Arquivo, ela não iniciará seu funcionamento ao inicializar o sistema operacional. Você precisará reativar manualmente a Proteção Contra Ameaças ao Arquivo.

Ativar/desativar a Proteção Contra Ameaças ao Arquivo

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças ao Arquivo**, marque/desmarque a caixa de seleção **Ativar Proteção Contra Ameaças ao Arquivo**.

   Você também pode ativar a Proteção Contra Ameaças ao Arquivo no Centro de Proteção. Desativar a proteção do computador ou os componentes de proteção aumenta consideravelmente o risco de infecção do seu computador. É por isso que o Centro de Proteção lhe informa quando a proteção do computador estiver desativada.

É possível criar um escopo de proteção para a Proteção Contra Ameaças ao Arquivo.

Adicionar/remover um arquivo ou uma pasta do escopo de proteção

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças ao Arquivo**, clique em Escopo da proteção.

   Será exibida uma janela com uma lista dos objetos que serão verificados pela Proteção Contra Ameaças ao Arquivo. Por padrão, a Proteção Contra Ameaças ao Arquivo verifica todos os objetos localizados nos discos internos, removíveis e conectados da rede ao computador.

   > **Nota:** é possível ignorar a verificação do volume do sistema somente leitura para reduzir significativamente o tempo de verificação. Por padrão, a Proteção Contra Ameaças ao Arquivo não verifica o volume do sistema somente leitura.

3. Na seção **Escopo da proteção**, adicione/remova os objetos ao/do escopo da proteção:

   - Para adicionar um arquivo ou uma pasta ao escopo de proteção:

     a. Clique em +.

     Será exibida um menu suspenso no qual você poderá selecionar os objetos que deseja adicionar ao escopo de proteção.

     b. No menu suspenso, escolha o item **Arquivos e pastas**.

     Será exibida uma caixa de diálogo na qual você poderá selecionar um arquivo ou uma pasta.

     c. Selecione o arquivo ou a pasta que deseja adicionar ao escopo de proteção.

     d. Clique em **Abrir**.

- Para remover um arquivo ou uma pasta do escopo de proteção:

  a. Selecione um objeto na lista de objetos do escopo de proteção.

  b. Arraste o objeto selecionado da janela ou clique –.

4. Se deseja verificar o volume do sistema somente leitura, na seção **Otimização**, desmarque a caixa de seleção **Ignorar a verificação de volumes de sistema somente leitura**.

> **Importante:** a otimização pode estar desativada por motivos de segurança.

5. Clique em **Salvar**.

Adicionar/remover um objeto na lista de objetos padrão para/de o escopo de proteção

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças ao Arquivo**, clique em Escopo da proteção.

   Será exibida uma janela com uma lista dos objetos que serão verificados pela Proteção Contra Ameaças ao Arquivo. Por padrão, a Proteção Contra Ameaças ao Arquivo verifica todos os objetos localizados nos discos internos, removíveis e conectados da rede ao computador.

> **Nota:** é possível ignorar a verificação do volume do sistema somente leitura para reduzir significativamente o tempo de verificação. Por padrão, a Proteção Contra Ameaças ao Arquivo não verifica o volume do sistema somente leitura.

3. Na seção **Escopo da proteção**, adicione/remova os objetos na lista de objetos padrão ao/do escopo da proteção:

   - Para adicionar um objeto na lista de objetos padrão para o escopo de proteção:

     a. Clique em +.

     Será exibida um menu suspenso no qual você poderá selecionar os objetos que deseja adicionar ao escopo de proteção.

     b. No menu suspenso, selecione um objeto que será adicionado ao escopo de proteção (por exemplo, **Todos os discos internos**).

   - Para remover um objeto da lista de objetos padrão do escopo de proteção:

     a. Selecione um objeto na lista de objetos do escopo de proteção.

     b. Arraste o objeto selecionado da janela ou clique –.

4. Se deseja verificar o volume do sistema somente leitura, na seção **Otimização**, desmarque a caixa de seleção **Ignorar a verificação de volumes de sistema somente leitura**.

> **Importante:** a otimização pode estar desativada por motivos de segurança.

5. Clique em **Salvar**.

Desativar a proteção de um objeto no escopo de proteção

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças ao Arquivo**, clique em Escopo da proteção.

   Será exibida uma janela com uma lista dos objetos que serão verificados pela Proteção Contra Ameaças ao Arquivo. Por padrão, a Proteção Contra Ameaças ao Arquivo verifica todos os objetos localizados nos discos internos, removíveis e conectados da rede ao computador.

   Nota: é possível ignorar a verificação do volume do sistema somente leitura para reduzir significativamente o tempo de verificação. Por padrão, a Proteção Contra Ameaças ao Arquivo não verifica o volume do sistema somente leitura.

3. Desmarque a caixa de seleção ao lado de um objeto na lista de objetos do escopo de proteção.

4. Clique em **Salvar**.

Ativar a verificação do volume do sistema somente leitura

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças ao Arquivo**, clique em Escopo da proteção.

   Será exibida uma janela com uma lista dos objetos que serão verificados pela Proteção Contra Ameaças ao Arquivo. Por padrão, a Proteção Contra Ameaças ao Arquivo verifica todos os objetos localizados nos discos internos, removíveis e conectados da rede ao computador.

   Nota: é possível ignorar a verificação do volume do sistema somente leitura para reduzir significativamente o tempo de verificação. Por padrão, a Proteção Contra Ameaças ao Arquivo não verifica o volume do sistema somente leitura.

3. Na seção **Otimização**, desmarque a caixa de seleção **Ignorar a verificação de volumes de sistema somente leitura**.

   Importante: a otimização pode estar desativada por motivos de segurança.

4. Clique em **Salvar**.

Quando você ou um aplicativo tenta acessar um arquivo incluído no escopo da proteção, a Proteção Contra Ameaças ao Arquivo verifica os bancos de dados iSwift quanto a informações sobre esse arquivo e usa essas informações para decidir se é necessário verificar o arquivo.

O reconhecimento de objetos maliciosos é possível graças ao uso da *análise de assinaturas*, um método de pesquisa de ameaças que se baseia em descrições de ameaças incluídas nos bancos de dados antimalware. Além da análise de assinaturas, a Proteção Contra Ameaças ao Arquivo usa a análise heurística e outras tecnologias de verificação.

Se uma ameaça for detectada em um arquivo, o Kaspersky Endpoint Security identifica o tipo de malware detectado (por exemplo, *vírus* ou *Cavalo de Troia*). Em seguida, o aplicativo exibe uma notificação sobre o objeto detectado e executa uma ação no objeto com base nas configurações de Proteção Contra Ameaças ao Arquivo.

Selecionar a ação executada pela Proteção Contra Ameaças ao Arquivo ao detectar um arquivo infectado

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção Proteção Contra Ameaças ao Arquivo, selecione a ação que a Proteção Contra Ameaças ao Arquivo executará ao detectar um arquivo infectado.

Antes de tentar desinfectar ou excluir um objeto infectado, o Kaspersky Endpoint Security salva uma cópia de backup para posterior restauração ou desinfecção.

As informações sobre o funcionamento da Proteção Contra Ameaças ao Arquivo e todos os objetos detectados são registradas em um relatório.

Nota: se a execução da Proteção Contra Ameaças ao Arquivo for interrompida com um erro, você poderá consultar o relatório e tentar reiniciar o componente. Se o problema não for resolvido, você pode entrar em contato com o Suporte Técnico da Kaspersky.

Exibir o relatório de Proteção Contra Ameaças ao Arquivo

1. Na barra de menus, selecione **Proteção** > **Relatórios**.

   Será exibida a janela **Relatórios**.

2. Abra a guia **Proteção Contra Ameaças ao Arquivo**.

Proteção Contra Ameaças da Web

Quando a Internet é usada, seu computador corre risco de infecção por malware e outras ameaças à segurança do computador. As ameaças à segurança do computador podem entrar no computador quando você baixa programas gratuitos ou visita sites que foram atacados por hackers. Além disso, os worms de rede podem atacar seu computador assim que o seu computador estabelecer uma conexão com a Internet, mesmo antes de abrir um endereço da Web ou baixar um arquivo.

O Kaspersky Endpoint Security protege as informações que o computador envia e recebe por meio de protocolos HTTP e HTTPS no Safari, Chrome ou Firefox.

Nota: o Kaspersky Endpoint Security monitora o tráfego da Web nas portas usadas com mais frequência para a transferência de dados por HTTP e HTTPS. O Kaspersky Endpoint Security verifica as conexões criptografadas (HTTPS) somente se a caixa de seleção **Verificar conexões seguras (HTTPS)** na seção **Geral** estiver marcada.

Ativar/desativar a Proteção Contra Ameaças da Web

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças da Web**, marque/desmarque a caixa de seleção **Ativar Proteção Contra Ameaças da Web**.

Você também pode ativar a Proteção Contra Ameaças da Web pelo Centro de Proteção. Desativar a proteção do computador ou os componentes de proteção aumenta consideravelmente o risco de infecção do seu computador. É por isso que o Centro de Proteção lhe informa quando a proteção do computador estiver desativada.

Importante: se você tiver desativado a Proteção Contra Ameaças da Web, a reativação não será feita automaticamente quando o Kaspersky Endpoint Security ou o sistema operacional forem reiniciados. Será necessário reativar manualmente a Proteção Contra Ameaças da Web.

A Proteção Contra Ameaças da Web verifica o tráfego da Web de acordo com as configurações recomendadas pela Kaspersky. Os objetos maliciosos são reconhecidos usando análise de assinatura, análise heurística e dados da Kaspersky Security Network.

A verificação de links em sites para detectar ameaças de phishing e endereços da Web maliciosos torna possível evitar *ataques de phishing*. Os *ataques de phishing* normalmente ocorrem na forma de mensagens de e-mail de criminosos que se passam por instituições financeiras (como bancos) e enviam links para sites fraudulentos. Nesses e-mails, os criminosos tentam persuadir o usuário a visitar um site de phishing e inserir dados confidenciais (como o número do seu cartão bancário ou o nome e a senha da sua conta de banco online). Um ataque de phishing pode ser disfarçado, por exemplo, como uma mensagem do seu banco com um link ao seu site oficial, que, na realidade, leva para uma cópia exata do site oficial do banco criado por impostores.

A Proteção Contra Ameaças da Web monitora o tráfego da Web para detectar tentativas de visitar um site de phishing e bloqueia o acesso a esses sites. Para verificar os links em sites em busca de ameaças de phishing e endereços da Web maliciosos, o Kaspersky Endpoint Security usa os bancos de dados do aplicativo, a análise heurística e os dados da Kaspersky Security Network.

Algoritmo de verificação do tráfego na Web

Cada site ou arquivo que você ou um aplicativo acessa através dos protocolos HTTP e HTTPS é interceptado e verificado pela Proteção Contra Ameaças da Web para detectar a presença de código malicioso:

- Se um site ou arquivo contiver um código malicioso, o Kaspersky Endpoint Security poderá bloqueá-lo e exibir uma notificação informando que ele está infectado.
- Se o arquivo ou o site não tiver código malicioso, você poderá acessá-lo imediatamente.

Selecione a ação que a Proteção Contra Ameaças da Web deve executar após detectar um objeto de tráfego da Web perigoso

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças da Web**, selecione a ação que a Proteção Contra Ameaças da Web deve executar ao detectar um objeto de tráfego da Web perigoso.

Informações sobre o funcionamento da Proteção Contra Ameaças da Web e todos os objetos perigosos detectados no tráfego da Web são registradas em um relatório.

Nota: se a execução da Proteção Contra Ameaças da Web for interrompida com um erro, você poderá consultar o relatório da Proteção Contra Ameaças da Web e tentar reiniciar o componente. Se o problema não for resolvido, você pode entrar em contato com o Suporte Técnico da Kaspersky.

Exibir o relatório de Proteção Contra Ameaças da Web

1. Na barra de menus, selecione **Proteção** > **Relatórios**.

   Será exibida a janela **Relatórios**.

2. Abra a guia **Proteção Contra Ameaças da Web**.

Proteção Contra Ameaças ao Correio

O componente Proteção Contra Ameaças ao Correio analisa os anexos de e-mails recebidos e enviados para identificar malwares e outras ameaças. O componente protege o computador usando bancos de dados antimalware, o serviço em nuvem da Kaspersky Security Network e a análise heurística.

O aplicativo é compatível com os seguintes clientes de e-mail: Apple Mail, Microsoft Outlook, Mozilla Thunderbird, Canary Mail, Spark, Mimestream, Airmail, Post Box, Boxy Suite 2, Twobird, Shift, Clean Email, eM Client, Superhuman, Polymail, HEY, Mail+ for Gmail, Spike mail.

Por padrão, a Proteção Contra Ameaças ao Correio está ativada. É possível desativar a Proteção Contra Ameaças ao Correio, se necessário.

Dependendo do modo de operação selecionado, a Proteção Contra Ameaças ao Correio executa as seguintes ações:

- **Exclua objetos maliciosos automaticamente**. Se essa opção estiver selecionada, quando o Kaspersky Endpoint Security detectar um objeto infectado em uma mensagem de e-mail, ele excluirá o objeto infectado e substituirá o conteúdo do objeto pelo texto "The requested file infected with <nome do vírus> has been deleted".

- **Bloqueie objetos maliciosos automaticamente**. Se essa opção estiver selecionada, quando o Kaspersky Endpoint Security detectar um objeto infectado em uma mensagem de e-mail, ele substituirá o assunto da mensagem por "Message is infected: <assunto original>" sendo <assunto original> o assunto original. O assunto da mensagem de e-mail só é substituído para o protocolo POP3.

Ativar/desativar a Proteção Contra Ameaças ao Correio usando o Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.

2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é aberta.

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

4. Vá para **Comunicação e Proteção na Web → Proteção Contra Ameaças ao Correio**.

5. Ative ou desative o componente usando o botão de alternância **Proteção Contra Ameaças ao Correio**.

6. Com a Proteção Contra Ameaças ao Correio ativada, selecione a ação que o aplicativo deve executar ao detectar malwares:

   - **Excluir**

   - **Bloquear**

7. Se necessário, na seção **Ajustes avançados**, defina o limite de tempo para a verificação de arquivos compactados ou o tamanho máximo do arquivo compactado para verificação.

8. Salve suas alterações.

Ativar/desativar a Proteção Contra Ameaças ao Correio usando o Console de Administração

1. Inicie o Console de Administração.

2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.

3. Na árvore do console, clique em **Dispositivos gerenciados**.

4. Na área de trabalho, selecione a guia **Políticas**.

5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.

6. Na janela **Propriedades**, selecione **Proteção Essencial Contra Ameaças** > **Proteção Contra Ameaças ao Correio**.

7. Marque ou desmarque a caixa **Ativar Proteção Contra Ameaças ao Correio**.

8. Na seção **Ação ao detectar ameaça**, selecione a ação a ser executada quando o Kaspersky Endpoint Security detectar uma ameaça.

9. Se necessário, na seção **Ajustes da Proteção Contra Ameaças ao Correio**, defina o tempo limite ou o tamanho máximo de arquivos compactados para verificação.

10. Clique em **OK** para salvar suas alterações.

11. Siga um destes procedimentos para aplicar as alterações à política:

    - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da política>** após salvar as alterações.

    - Clique em **OK** para fechar a janela **Propriedades: <Nome da política>** após salvar as alterações.

Ative/desative a Proteção Contra Ameaças ao Correio pelo aplicativo Kaspersky Endpoint Security

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças ao Correio**, marque/desmarque a caixa **Ativar Proteção Contra Ameaças ao Correio**.

3. Se a caixa **Ativar Proteção Contra Ameaças ao Correio** estiver marcada, selecione a ação a ser executada quando o Kaspersky Endpoint Security detectar uma ameaça.

4. Se necessário, defina o limite de tempo para a verificação de arquivos compactados ou o tamanho máximo do arquivo compactado para verificação.

Exibir o relatório de Proteção Contra Ameaças ao Correio

1. Na barra de menus, selecione **Proteção** > **Relatórios**.

   Será exibida a janela **Relatórios**.

2. Abra a guia **Proteção Contra Ameaças ao Correio**.

Proteção Contra Ameaças à Rede

O Kaspersky Endpoint Security protege o seu computador contra ataques à rede.

Um *ataque à rede* é uma tentativa de invadir o sistema operacional de um computador remoto. Os criminosos tentam ataques à rede para estabelecer controle sobre o sistema operacional, causando recusa de serviço no sistema operacional ou acessando informações sigilosas. Para alcançar esses objetivos, os criminosos executam ataques diretos, como a verificação de portas e ataques de força bruta, ou usam malwares instalados no computador que está sendo atacado.

Os ataques à rede podem ser divididos nos seguintes tipos:

- *Verificar portas*. Esse tipo de ataque à rede é normalmente executado como preparação de um ataque de rede mais perigoso. Um intruso verifica portas UDP/TCP que usam serviços de rede no computador-alvo e determina a vulnerabilidade do computador-alvo a outros tipos de ataques à rede mais perigosos. A verificação de portas também permite que o intruso determine o sistema operacional do computador-alvo e selecione os ataques à rede adequados para tal sistema operacional.

- *Ataques DoS* ou ataques à rede que causam uma recusa de serviço. Esse tipo de ataques à rede torna o sistema operacional-alvo instável ou totalmente inutilizável.

  Os principais tipos de ataques DoS são:

  - A transmissão de pacotes de rede especialmente projetados e não esperados pelo computador-alvo que causam, portanto, o funcionamento incorreto ou erro fatal do sistema operacional-alvo.

  - O envio de um grande número de pacotes de rede para um computador remoto em um curto período de tempo. Todos os recursos do computador-alvo são usados para processar os pacotes de rede enviados pelo intruso. Como resultado, o computador deixa de executar as suas funções.

- *Ataques de intrusão de rede*. Estes ataques à rede são projetados para "sequestrar" o sistema operacional do computador-alvo. Este é o tipo de ataque à rede mais perigoso, pois, caso tenha êxito, o intruso obtém controle total sobre o sistema operacional.

  Este tipo de ataque à rede é usado quando o intruso deseja obter dados confidenciais (tais como números de cartões bancários ou senhas) de um computador remoto ou usar secretamente o computador remoto para atingir seus objetivos (por exemplo, atacar outros computadores a partir desse computador).

Ativar/desativar a Proteção Contra Ameaças à Rede

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças à Rede**, marque/desmarque a caixa de seleção **Ativar Proteção Contra Ameaças à Rede**.

Você também pode ativar a Proteção Contra Ameaças à Rede no Centro de Proteção. Desativar a proteção do computador ou os componentes de proteção aumenta consideravelmente o risco de infecção do seu computador. É por isso que o Centro de Proteção lhe informa quando a proteção do computador estiver desativada.

Importante: se você tiver desativado a Proteção Contra Ameaças à Rede, a reativação não será feita automaticamente quando o Kaspersky Endpoint Security ou o sistema operacional forem reiniciados. Você precisará ativar novamente a Proteção Contra Ameaças à Rede manualmente.

Quando o aplicativo detecta a atividade de rede perigosa, o Kaspersky Endpoint Security automaticamente adiciona o endereço IP do computador responsável pelo ataque à lista de computadores bloqueados, a menos que esse computador esteja na lista de computadores confiáveis.

Editar a lista de computadores bloqueados

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças à Rede**, marque a caixa de seleção **Ativar Proteção Contra Ameaças à Rede**.

3. Clique em **Ajustes**.

   Será exibida uma janela com uma lista de computadores confiáveis e uma lista de computadores bloqueados.

4. Abra a guia **Computadores bloqueados**.

5. Se você tiver certeza de que o computador bloqueado não é uma ameaça, selecione o endereço IP do computador na lista e clique em **Desbloquear**.

   Será exibida uma caixa de diálogo de confirmação.

6. Na janela de confirmação, siga um destes procedimentos:

   - Se você desejar desbloquear o computador, clique em **Desbloquear**.

     O Kaspersky Endpoint Security desbloqueia o endereço IP.

   - Se você deseja que o Kaspersky Endpoint Security nunca bloqueie o endereço IP selecionado, clique **Desbloquear e excluir**.

     O Kaspersky Endpoint Security desbloqueará o endereço IP e o adicionará à lista de computadores confiáveis.

7. Clique em **Salvar**.

Você pode criar e editar a lista de computadores confiáveis. O aplicativo Kaspersky Endpoint Security não bloqueará os endereços IP desses computadores automaticamente, mesmo se for detectada uma atividade de rede perigosa associada a eles.

Editar a lista de computadores confiáveis

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Essencial**, na seção **Proteção Contra Ameaças à Rede**, marque a caixa de seleção **Ativar Proteção Contra Ameaças à Rede**.

3. Clique em **Ajustes**.

   Será exibida uma janela com uma lista de computadores confiáveis e uma lista de computadores bloqueados.

4. Abra a guia **Computadores confiáveis**.

5. Edite a lista de computadores confiáveis:

   - Para adicionar um endereço IP à lista de computadores confiáveis:

     a. Clique em +.

     b. Clique no campo para ser exibido e insira o endereço IP do computador que você considera confiável.

   - Para remover um endereço IP da lista de computadores confiáveis:

     a. Selecione um endereço IP na lista.

     b. Clique em –.

   - Para editar um endereço IP na lista de computadores confiáveis:

     a. Selecione um endereço IP na lista.

     b. Clique em **Editar**.

     c. Altere o endereço IP.

6. Clique em **Salvar**.

Quando um ataque à rede for detectado, o Kaspersky Endpoint Security registrará informações sobre o ataque em um relatório.

Nota: se a execução do componente Proteção Contra Ameaças à Rede for interrompida com um erro, você poderá ver o relatório e tentar reiniciar o componente. Se o problema não for resolvido, você pode entrar em contato com o Suporte Técnico da Kaspersky.

Exibir o relatório de Proteção Contra Ameaças à Rede

1. Na barra de menus, selecione **Proteção** > **Relatórios**.

   Será exibida a janela **Relatórios**.

2. Abra a guia **Proteção Contra Ameaças à Rede**.

Firewall

O Firewall bloqueia as conexões não autorizadas com o computador durante o trabalho na Internet ou rede local. Isso permite proteger sua LAN contra roubo de identidade e outros ataques. O componente oferece proteção ao computador com a ajuda de bancos de dados antimalware, do serviço em nuvem da Kaspersky Security Network e de regras de rede predefinidas.

Prioridades de regras de rede

Cada regra tem uma prioridade. Quanto mais alta uma regra estiver na lista, mais alta será sua prioridade. Se a atividade de rede for adicionada a várias regras, o Firewall regulará a atividade de rede de acordo com a regra com a prioridade mais alta.

Tipos de conexão de rede

O Firewall permite controlar a atividade da rede, dependendo do tipo de conexão de rede. Você pode alterar o tipo de conexão de rede nas configurações do Kaspersky Endpoint Security.

Os seguintes tipos de conexão de rede estão disponíveis:

- **Rede pública**. A rede não está protegida por aplicativos antimalware, firewalls ou filtros (como Wi-Fi em um café). Quando o usuário opera um computador conectado a essa rede, o Firewall bloqueia o acesso a arquivos e impressoras desse computador. Os usuários externos também não podem acessar dados por meio de pastas compartilhadas e acesso remoto à área de trabalho deste computador. O Firewall atribui o tipo de rede Pública à Internet por padrão. Você não pode alterar o tipo da Internet.

- **Rede local**. Rede para usuários com acesso restrito a arquivos e impressoras neste computador (como para uma LAN ou rede doméstica).

- **Rede confiável**. Rede segura na qual o computador não é exposto a ataques ou tentativas não autorizadas de acesso a dados. O Firewall permite qualquer atividade de rede dentro de redes com esse status.

Gerenciar o componente Firewall no Console de Administração

1. Inicie o Console de Administração.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Na área de trabalho, selecione a guia **Políticas**.
5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
6. Na janela **Propriedades**, selecione **Proteção Essencial Contra Ameaças** > **Firewall**.
7. Marque ou desmarque a caixa de seleção **Ativar Firewall**.
8. Na seção **Configurações do Firewall**, clique no botão **Ajustes** e adicione, edite, exclua ou altere a prioridade das regras.
9. Na seção **Redes disponíveis**, clique no botão **Ajustes** e adicione, edite, exclua ou altere o tipo das redes.
10. Clique em **OK** para salvar suas alterações.

11. Siga um destes procedimentos para aplicar as alterações à política:

    - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da política>** após salvar as alterações.
    - Clique em **OK** para fechar a janela **Propriedades: <Nome da política>** após salvar as alterações.

Gerenciar o componente Firewall no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Comunicação e Proteção na Web** → **Firewall**.
5. Ative ou desative o componente usando o botão de alternância **Firewall**.
6. Na seção **Configurações do Firewall**, clique no botão **Regras de pacotes de rede** e adicione, edite, exclua ou altere a prioridade das regras.
7. Na seção **Redes disponíveis**, clique no botão **Configurações de rede** e adicione, edite ou altere o tipo das redes.
8. Salve suas alterações.

Gerenciar o componente Firewall no aplicativo Kaspersky Endpoint Security

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.
2. Na guia **Essencial**, na seção **Firewall**, desmarque/marque a caixa de seleção **Ativar Firewall**.
3. Se necessário, clique no botão **Ajustes** e defina as configurações do Firewall:

    - Na guia **Regras do pacote de rede**, você pode adicionar, editar, excluir ou alterar a prioridade das regras.
    - Na guia **Redes disponíveis**, você pode adicionar, editar ou alterar o tipo das redes.

Como resultado, se o Firewall estiver ativado, o Kaspersky Endpoint Security controla a atividade de rede e bloqueia conexões de rede não autorizadas ao computador.

Visualizar o relatório do Firewall

1. Na barra de menus, selecione **Proteção** > **Relatórios**.

   Será exibida a janela **Relatórios**.
2. Abra a guia **Firewall**.

Detecção de Comportamento

O componente Detecção de Comportamento recebe dados sobre as ações dos aplicativos em seu computador e fornece essas informações a outros componentes de proteção para melhorar o desempenho. O componente Detecção de Comportamento usa Assinaturas de Fluxo de Comportamento (BSS) dos aplicativos. Caso a atividade de um aplicativo corresponda a uma assinatura de fluxo de comportamento, o Kaspersky Endpoint Security executará a ação de resposta selecionada. A funcionalidade do Kaspersky Endpoint Security com base em padrões de atividades perigosas fornece Defesa Proativa ao computador.

Por padrão, a Detecção de Comportamento é ativada e executada no modo recomendado pelos especialistas da Kaspersky. É possível desativar a Detecção de Comportamento, caso necessário.

Ativar/desativar a Detecção de Comportamento pelo Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para a seção **Proteção Contra Ameaças ao Host → Análise de comportamento → Detecção de Comportamento**.
5. Ative ou desative o componente usando o botão de alternância **Detecção de Comportamento**.
6. Caso a Detecção de Comportamento esteja ativada, selecione uma das seguintes ações a ser executada quando a atividade de malware for detectada:

   - **Bloquear**

     Caso esta opção seja selecionada, o aplicativo Kaspersky Endpoint Security encerrará o aplicativo ao detectar a atividade maliciosa.

   - **Excluir**

     Caso esta opção seja selecionada, o Kaspersky Endpoint Security excluirá o arquivo executável de um aplicativo malicioso e criará uma cópia backup do arquivo no Backup quando uma atividade maliciosa for detectada.

   - **Perguntar o que fazer**

     Caso esta opção esteja selecionada, quando a atividade de malware for detectada, o aplicativo Kaspersky Endpoint Security exibirá uma janela de notificação com as informações sobre o objeto malicioso e solicitará que o usuário escolha a ação a ser executada pelo aplicativo Kaspersky Endpoint Security. As ações disponíveis podem variar dependendo do status do objeto.
7. Se a Detecção e Proteção de Comportamento de pastas compartilhadas contra criptografia externa estiverem ativadas, selecione uma das seguintes ações a serem executadas ao detectar a criptografia externa:

   - **Informar**

     Se esta opção for selecionada, ao detectar uma tentativa de modificação de arquivos em pastas compartilhadas, o aplicativo Kaspersky Endpoint Security registrará informações sobre esta tentativa na lista de ameaças ativas, adicionará uma entrada nos relatórios do aplicativo local e enviará informações sobre a atividade maliciosa detectada para o Kaspersky Security Center.

- **Bloquear o dispositivo invasor para**

  Se esta opção for selecionada, quando o aplicativo Kaspersky Endpoint Security detectar uma tentativa de modificação de arquivos em pastas compartilhadas, ele bloqueará o acesso à modificação do arquivo (somente leitura) para a sessão que iniciou a atividade maliciosa e criará cópias de backup dos arquivos modificados.

8. Salve suas alterações.

Ativar/desativar a Detecção de Comportamento pelo Console de Administração

1. Inicie o Console de Administração.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Na área de trabalho, selecione a guia **Políticas**.
5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
6. Na janela **Propriedades**, selecione **Proteção Avançada Contra Ameaças** > **Detecção de Comportamento**
7. Marque ou desmarque a caixa de seleção **Ativar Detecção de Comportamento**.
8. Caso necessário, na seção **Ação ao detectar atividade de malware**, selecione a ação a ser executada quando a atividade de malware for detectada.
9. Clique em **OK** para salvar suas alterações.
10. Siga um destes procedimentos para aplicar as alterações à política:

    - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da política>** após salvar as alterações.
    - Clique em **OK** para fechar a janela **Propriedades: <Nome da política>** após salvar as alterações.

Ative/desative a Detecção de Comportamento pelo aplicativo Kaspersky Endpoint Security

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.
2. Na guia **Avançado**, na seção **Detecção de Comportamento**, marque ou desmarque a caixa de seleção **Ativar Detecção de Comportamento**.
3. Caso a caixa de seleção **Ativar Detecção de Comportamento** estiver marcada, selecione uma das seguintes ações a ser executada quando a atividade de malware for detectada:

    - **Bloquear**

      Caso esta opção seja selecionada, o aplicativo Kaspersky Endpoint Security encerrará o aplicativo ao detectar a atividade maliciosa.

    - **Excluir**

      Caso esta opção seja selecionada, o Kaspersky Endpoint Security excluirá o arquivo executável de um aplicativo malicioso e criará uma cópia backup do arquivo no Backup quando uma atividade maliciosa for detectada.

- **Perguntar o que fazer**

  Caso esta opção esteja selecionada, quando a atividade de malware for detectada, o aplicativo Kaspersky Endpoint Security exibirá uma janela de notificação com as informações sobre o objeto malicioso e solicitará que o usuário escolha a ação a ser executada pelo aplicativo Kaspersky Endpoint Security. As ações disponíveis podem variar dependendo do status do objeto.

Assim, caso a Detecção de Comportamento esteja ativada, o Kaspersky Endpoint Security usará as assinaturas de fluxo de comportamento para analisar a atividade dos aplicativos no sistema operacional.

Importante: não recomendamos desativar a Detecção de Comportamento, a menos que seja absolutamente necessário, pois isso reduzirá a eficácia dos componentes de proteção. Para detectar ameaças, os componentes de proteção podem solicitar dados coletados pelo componente Detecção de Comportamento.

Verificação

A Proteção Contra Ameaças ao Arquivo e a Proteção Contra Ameaças da Web fornecem proteção do computador em tempo real. Também recomendamos verificar regularmente o computador em busca de malware e outras ameaças de segurança do computador. A verificação do computador é necessária para impedir a disseminação de malwares que não foram detectados pelos componentes de proteção.

O Kaspersky Endpoint Security contém as seguintes tarefas de verificação integradas:

- **Verificação completa**.

  Uma verificação de malware da memória, objetos de inicialização e todos os discos internos do computador.

- **Verificação rápida**.

  Uma verificação de malware apenas nas áreas mais importantes do computador: memória, objetos de inicialização e pastas do sistema.

- **Verificação personalizada**.

  Uma verificação de malware de um objeto especificado (arquivo, pasta, disco interno ou removível).

- **Verificação dos discos externos**

  Uma verificação de malware nos discos externos realizada quando um disco externo é conectado ao computador.

Quando o aplicativo executa uma tarefa de verificação, objetos maliciosos são reconhecidos através da análise de assinaturas. Além da análise de assinaturas, o Kaspersky Endpoint Security usa a análise heurística e outras tecnologias de verificação.

A janela **Verificação** exibe informações sobre o andamento de cada tarefa de verificação em execução (porcentagem concluída e tempo restante), além do histórico de verificação (100 tarefas de verificação mais recentes).

Iniciar tarefas de verificação completa e verificação rápida

1. Na barra lateral da janela principal do aplicativo, clique em **Verificação**.
   Será exibida a janela **Verificação**.
2. Na janela **Verificação**, clique no botão **Verificação completa** ou **Verificação rápida**.

A tarefa de verificação será iniciada.

Iniciar uma tarefa de Verificação Personalizada

1. Na barra lateral da janela principal do aplicativo, clique em **Verificação**.
   Será exibida a janela **Verificação**.
2. Para iniciar a tarefa **Verificação personalizada**, siga um destes procedimentos:
   - Arraste um arquivo ou pasta para a janela.
   - Clique em **Escolher** e abra um arquivo ou pasta.

A tarefa de verificação será iniciada.

Parar uma tarefa de verificação

1. Na barra lateral da janela principal do aplicativo, clique em **Verificação**.
   Será exibida a janela **Verificação**.
2. Na janela **Verificação**, clique no botão Parar ( ) ao lado da tarefa de verificação que deseja parar.
   Será exibida uma caixa de diálogo de confirmação.
3. Na caixa de diálogo de confirmação, clique **Parar**.

A tarefa de verificação será interrompida.

Você pode agendar a tarefa de Verificação Rápida ou uma tarefa de Verificação Completa.

Programar uma tarefa de verificação na janela Verificação

1. Na barra lateral da janela principal do aplicativo, clique em **Verificação**.
   Será exibida a janela **Verificação**.
2. Clique em **Agendar a verificação**.
   Uma caixa de diálogo é aberta onde você poderá definir o agendamento.
3. Selecione a caixa de seleção **Verificação completa** ou **Verificação rápida**.
4. Especifique a frequência de verificação e o horário do início da verificação.
5. Clique em **OK**.

Programar uma tarefa de verificação na janela Configurações

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.
   É aberta a janela de ajustes do aplicativo.

2. Na guia **Verificação**, clique em **Agendamento**.

3. Na janela que se abre, marque a caixa de seleção ao lado do nome da tarefa de verificação que você deseja iniciar em uma programação.

4. Configure a frequência e a hora da tarefa de verificação.

5. Clique em **OK** para salvar as alterações feitas no agendamento da tarefa de verificação.

Quando um disco externo é conectado ao computador, o aplicativo Kaspersky Endpoint Security pode iniciar a verificação do disco automaticamente, solicitar autorização para verificar ou não fazer nada. É possível selecionar uma das opções nas configurações da tarefa Verificação dos discos externos.

Selecione a ação que o aplicativo Kaspersky Endpoint Security deve executar quando um disco externo for conectado ao computador

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Verificação**, na lista à esquerda, selecione a tarefa **Verificação dos discos externos**.

3. Na seção **Quando um disco externo for conectado**, selecione a ação que o Kaspersky Endpoint Security deve executar quando um disco externo for conectado.

As tarefas de Verificação Completa e Verificação Rápida já contêm os escopos de verificação. Durante a execução da tarefa de Verificação Completa, o aplicativo Kaspersky Endpoint Security verifica a memória, os objetos de inicialização e todos os discos internos do computador. Durante a execução da tarefa de Verificação Rápida, o aplicativo verifica a memória do computador, os objetos de inicialização e as pastas do sistema. Você pode alterar o escopo de verificação da tarefa de Verificação Rápida.

Nota: é possível ignorar a verificação do volume do sistema somente leitura para reduzir significativamente o tempo de verificação. Por padrão, o Kaspersky Endpoint Security não verifica o volume do sistema somente leitura, ao executar uma tarefa de Verificação Rápida, e o verifica ao executar uma tarefa de Verificação Completa.

Nota: o Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.

Ativar/desativar a verificação do volume do sistema somente leitura

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Verificação**, na lista à esquerda, selecione a tarefa **Verificação completa** ou **Verificação rápida**.

3. Na seção **Otimização**, desmarque/marque a caixa de seleção **Ignorar a verificação de volumes de sistema somente leitura**.

   Importante: a otimização pode estar desativada por motivos de segurança.

Adicionar/remover um arquivo ou uma pasta do escopo de verificação da tarefa de Verificação Rápida

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Verificação**, na lista à esquerda, selecione a tarefa **Verificação rápida**.

3. Na seção **Escopo da verificação**, clique **Editar**.

   Será exibida uma janela com a lista de objetos do escopo de verificação da tarefa Verificação Rápida.

4. Edite a lista de objetos do escopo da verificação:

   - Para adicionar um arquivo ou uma pasta ao escopo de verificação da tarefa Verificação Rápida:

     a. Clique em +.

     Um menu suspenso é exibido, no qual é possível selecionar os objetos que deseja adicionar ao escopo da verificação.

     b. Selecione o item **Arquivos e pastas**.

     Será exibida uma caixa de diálogo na qual você poderá selecionar um arquivo ou uma pasta.

     c. Selecione o arquivo ou a pasta que deseja adicionar ao escopo de verificação da tarefa Verificação Rápida.

     d. Clique em **Abrir**.

   - Para remover um arquivo ou uma pasta do escopo de verificação da tarefa Verificação Rápida:

     a. Selecione o objeto que deseja remover.

     b. Arraste o objeto selecionado da janela ou clique –.

5. Clique em **Salvar**.

Adicionar um objeto na lista de padrão da Verificação Rápida para o escopo de verificação da tarefa de Verificação Rápida

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Verificação**, na lista à esquerda, selecione a tarefa **Verificação rápida**.

3. Na seção **Escopo da verificação**, clique **Editar**.

   Uma janela com a lista de objetos do escopo de verificação será aberta.

4. Clique em +.

   Um menu suspenso é exibido, no qual é possível selecionar os objetos que deseja adicionar ao escopo da verificação.

5. No menu suspenso, selecione o objeto que deseja adicionar ao escopo da verificação (por exemplo, **Memória**).

6. Clique em **OK**.

Desativar a proteção de um objeto no escopo de verificação da tarefa Verificação Rápida

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Verificação**, na lista à esquerda, selecione a tarefa **Verificação rápida**.

3. Na seção **Escopo da verificação**, clique **Editar**.

   Uma janela com a lista de objetos do escopo de verificação será aberta.

4. Desmarque a caixa de seleção ao lado do objeto na lista de objetos do escopo da verificação.

5. Clique em **OK**.

Se uma ameaça for detectada em um arquivo, o aplicativo exibe uma notificação e executa a ação especificada no objeto. Você pode modificar a ação que é executada quando um objeto é detectado.

Selecione a ação que o Kaspersky Endpoint Security deve executar após detectar arquivos infectados

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Verificação**, selecione uma tarefa na lista.

3. Na seção **Ação**, selecione a ação que o aplicativo executará após detectar arquivos infectados.

Antes de desinfectar ou excluir um arquivo infectado, o Kaspersky Endpoint Security salva uma cópia dele no Backup, para que você possa restaurar o arquivo original, conforme necessário.

As informações sobre os resultados das tarefas de verificação e todos os objetos detectados são registradas em um relatório.

Nota: se ocorrer algum erro durante a execução da tarefa de verificação de malware, inicie a tarefa novamente. Se a nova tentativa de executar a verificação também resultar em um erro, entre em contato com o Suporte Técnico da Kaspersky.

Exibir o relatório da tarefa de verificação

1. Na barra de menus, selecione **Proteção** > **Relatórios**.

   Será exibida a janela **Relatórios**.

2. Abra a guia **Verificação**.

Tarefas de atualização

Atualizações regulares dos bancos de dados do aplicativo garantem que o computador esteja sempre protegido. A Proteção Contra Ameaças ao Arquivo, a Proteção Contra Ameaças da Web e as tarefas de verificação usam os bancos de dados do aplicativo para detectar e neutralizar malware no computador. Os bancos de dados do aplicativo são frequentemente atualizados com diferentes tipos de ameaças e maneiras de neutralizá-las, por isso é importante atualizá-los regularmente.

O Kaspersky Endpoint Security baixa os bancos de dados e novos módulos do aplicativo dos servidores de atualização Kaspersky e os instala no computador. O Kaspersky Endpoint Security também pode usar pontos de distribuição, pastas locais ou outros servidores da Web.

Nota: é necessário acesso à Internet para conectar-se aos servidores de atualização e baixar as atualizações. Se você se conectar à Internet por meio de um servidor proxy, poderá ser necessário definir as configurações de rede.

As atualizações dos bancos de dados do aplicativo podem ser baixadas de uma das seguintes maneiras:

- **Automaticamente**. O Kaspersky Endpoint Security verifica regularmente se há atualizações nos servidores de atualização Kaspersky. Se uma nova atualização estiver disponível no servidor de atualização, o Kaspersky Endpoint Security baixa a atualização em segundo plano e a instala no seu computador. Essa opção está ativada por padrão.

- **Manualmente**. É possível verificar manualmente se há atualizações do Kaspersky Endpoint Security a qualquer momento.

Ativar/desativar downloads automáticos de atualizações dos bancos de dados do Kaspersky Endpoint Security

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Atualização**, na seção **Bancos de dados**, marque/desmarque a caixa de seleção **Baixar atualizações automaticamente**.

Verificar se há atualizações de bancos de dados do Kaspersky Endpoint Security

1. Na barra lateral da janela principal do aplicativo, clique em **Atualização**.

   Será exibida a janela **Atualização**.

2. Clique em **Atualizar**.

O aplicativo começa a atualizar os bancos de dados.

Também é possível iniciar uma tarefa de atualização de uma das seguintes maneiras:

- Clique no ícone do aplicativo e escolha **Atualização**.

- Na barra de menus, selecione Proteção > **Atualização**.

Durante uma atualização, os bancos de dados e módulos do aplicativo são comparados com aqueles disponíveis atualmente nos servidores de atualização. Se a versão mais recente dos bancos de dados estiver instalada no computador, a janela **Atualização** exibirá uma mensagem para informar que os bancos de dados do aplicativo estão atualizados. Se a versão e os bancos de dados do aplicativo forem diferentes daqueles disponíveis atualmente no servidores de atualização, apenas os componentes ausentes da atualização serão baixados e instalados no computador. As atualizações incrementais dos bancos de dados do aplicativo levam menos tempo e exigem menos tráfego da Internet.

Se você se conectar à Internet por meio de um servidor proxy, poderá definir as configurações de conexão do servidor proxy. O Kaspersky Endpoint Security usa essas configurações para atualizar os bancos de dados do aplicativo e baixar atualizações dos módulos do aplicativo.

Configurar uma conexão com um servidor proxy

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Selecione a guia **Atualização**.

3. Na seção **Proxy**, marque a caixa de seleção **Usar servidor proxy** e clique em **Ajustes**.

   Uma janela é aberta, na qual você pode definir as configurações de conexão do servidor proxy.

4. Configure a conexão com um servidor proxy.

5. Clique em **Salvar** para salvar as alterações feitas nas configurações de conexão do servidor proxy.

Antes de atualizar os bancos de dados do aplicativo, o Kaspersky Endpoint Security cria cópias de backup deles para que uma reversão possa ser executada, conforme necessário. O recurso de reversão será útil se uma versão nova dos bancos de dados do aplicativo contiver uma assinatura incorreta que faz com que o Kaspersky Endpoint Security bloqueie um aplicativo seguro.

Nota: se os bancos de dados do Kaspersky Endpoint Security forem corrompidos, recomendamos que você inicie uma atualização para baixar e instalar a versão mais recente dos bancos de dados do aplicativo.

Reverter a última atualização

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Selecione a guia **Atualização**.

3. Na seção **Reversão**, clique em **Reverter atualização**.

O Kaspersky Endpoint Security também oferece um relatório detalhado sobre os resultados das tarefas de atualização na janela **Relatórios**.

Ver o relatório de uma tarefa de atualização

1. Na barra de menus, selecione **Proteção** > **Relatórios**.

2. Será exibida a janela **Relatórios**.

3. Selecione a guia **Atualização do banco de dados**.

Observação: A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinaturas de antimalware e atualizações de base de código), bem como a funcionalidade KSN, podem não estar disponíveis no software nos EUA.

Tarefas locais

Tarefa de verificação dos discos externos

O Kaspersky Endpoint Security pode verificar todos os arquivos executados ou copiados, mesmo se o arquivo estiver localizado em um disco externo. Para impedir a disseminação de malware, você pode configurar verificações automáticas de discos externos quando eles estiverem conectados ao dispositivo.

Os seguintes ajustes de Verificação de Discos Externos podem ser definidos:

- **A ação que o Kaspersky Endpoint Security executa quando um disco externo é conectado.**

  Verificação

  Se essa opção for selecionada, o Kaspersky Endpoint Security iniciará uma tarefa de verificação de malware para o disco externo conectado.

  Esta opção está marcada por padrão.

  Nenhuma ação

  Se essa opção estiver selecionada, o Kaspersky Endpoint Security não verificará o disco externo conectado.

- **A ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto malicioso.**

  Desinfectar e excluir se a desinfecção falhar

  Se essa opção estiver selecionada, o Kaspersky Endpoint Security bloqueará o acesso ao objeto infectado e tentará a desinfecção sem solicitar confirmação do usuário.

  Se o objeto for desinfetado, o Kaspersky Endpoint Security o salvará no local original com o nome do arquivo original. Se a desinfecção falhar, o Kaspersky Endpoint Security excluirá os objetos infectados que não puderam ser desinfetados.

  Esta opção está marcada por padrão.

  Perguntar o que fazer

  Se essa opção estiver selecionada, o Kaspersky Endpoint Security exibirá uma janela de notificação com informações sobre o objeto malicioso, e solicitará que o usuário escolha a ação a ser executada pelo Kaspersky Endpoint Security. As ações disponíveis podem variar dependendo do status do objeto.

Você pode configurar a Verificação de Discos Externos no Console de Administração, no Web Console ou no aplicativo Kaspersky Endpoint Security.

Como configurar a Verificação de Discos Externos no Console de Administração (MMC)

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Na área de trabalho, selecione a guia **Políticas**.
5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
6. Na janela **Propriedades**, selecione **Tarefas locais** > **Verificação dos discos externos**.

7. Definir os ajustes da tarefa.

8. Clique em **OK** para salvar suas alterações.

Como configurar a execução da Verificação de discos externos no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.

2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é aberta.

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

4. Vá para **Proteção Contra Ameaças ao Host → Verificação de unidades removíveis**.

5. Ative ou desative o componente usando o botão de alternância **Verificação de unidades removíveis**.

6. Salve suas alterações.

Como configurar a execução da Verificação de Discos Externos na interface do aplicativo

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Verificação**, na lista à esquerda, selecione a tarefa **Verificação dos discos externos**.

3. Na seção **Quando um disco externo for conectado**, selecione a ação que o Kaspersky Endpoint Security deve executar quando um disco externo for conectado.

Backup

Às vezes, a integridade dos arquivos infectados não pode ser preservada durante o processo de desinfecção. Se um arquivo desinfectado continha informação importante que fica parcialmente ou completamente inacessível após a desinfecção, você pode restaurar o arquivo original do Backup.

Uma *cópia de backup* é uma cópia de um arquivo perigoso criada quando o arquivo é desinfectado ou excluído. Ela é armazenada no Backup.

O *Backup* é uma área de armazenamento especial que contém cópias de backup dos arquivos que foram excluídos ou modificados durante a desinfecção. A função principal do Backup é a de permitir que o usuário restaure um arquivo original a qualquer momento. Os arquivos do Backup são salvos em um formato especial e não são perigosos para o computador.

Exibir o conteúdo do Backup

1. Na barra de menus, selecione **Proteção** > **Objetos detectados**.

   Será exibida a janela **Objetos detectados**.

2. Na seção **Efetuar backup**, visualize a lista de arquivos de backup.

Você pode restaurar ou remover cópias de backup dos arquivos do Backup.

Restaurar uma cópia de backup de um arquivo do Backup

1. Na barra de menus, selecione **Proteção** > **Objetos detectados**.

   Será exibida a janela **Objetos detectados**.

2. Na seção **Efetuar backup**, clique em ••• próximo ao arquivo que você deseja restaurar.

   O menu suspenso é aberto.

3. Selecione **Restaurar o arquivo**.

   Uma janela para especificar o nome do arquivo, a tag e a pasta na qual o arquivo será restaurado é aberta. Por padrão, o nome e o local do arquivo original já estão especificados.

4. Especifique o nome do arquivo e a pasta na qual ele será restaurado.

5. Clique em **Salvar**.

O aplicativo restaura o arquivo no local especificado com o nome especificado.

É necessário verificar o arquivo quanto à presença de malware imediatamente após restaurá-lo. É possível que o objeto possa ser desinfectado usando bancos de dados atualizados sem ser corrompido.

Importante: recomendamos que você não restaure cópias de segurança de arquivos a menos que a restauração seja absolutamente necessária, pois isso pode levar à infecção do computador.

Remover uma cópia de backup de um arquivo do Backup

1. Na barra de menus, selecione **Proteção** > **Objetos detectados**.

   Será exibida a janela **Objetos detectados**.

2. Na seção **Efetuar backup**, faça o seguinte:

   - Para excluir todas as cópias de backup de arquivos, clique em **Excluir tudo**.
   - Para excluir a cópia de backup selecionada, clique em ••• próximo a ela e escolha **Excluir cópia de backup**.

Por padrão, o período de armazenamento para arquivos no Backup é de 30 dias. Quando esse período expirar, os arquivos serão excluídos. Você pode alterar o período máximo de armazenamento de arquivos no Backup ou remover o limite do período de armazenamento.

Configurar o período de armazenamento de arquivos do Backup

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Ameaças**, na seção **Backup**, selecione a opção **Excluir backups de objetos após <number> dias** e especifique o período após o qual os arquivos armazenados no Backup serão excluídos automaticamente.

Relatórios

É possível visualizar um relatório do Kaspersky Endpoint Security que lista todos os objetos detectados na guia **Objetos processados**. Os eventos do sistema são exibidos na guia **Eventos do sistema**. Além disso, um relatório detalhado e separado é criado para cada um dos seguintes componentes de aplicativo: Proteção Contra Ameaças ao Arquivo, Proteção Contra Ameaças da Web, Proteção Contra Ameaças à Rede, Detecção de Comportamento e as tarefas de verificação e atualização.

Abrir a janela Relatórios

Na barra de menus, selecione **Proteção** > **Relatórios**.

O Kaspersky Endpoint Security pode salvar relatórios no formato de texto. Essa funcionalidade pode ser útil se as tarefas ou os componentes do aplicativo produzirem erros que você não consegue corrigir por conta própria, tornando necessária a ajuda do Suporte Técnico da Kaspersky. Nesse caso, envie o relatório em formato de texto para o Suporte Técnico da Kaspersky para que nossos especialistas possam investigar o problema e corrigi-lo o mais rápido possível.

Exportar um relatório de componente ou uma tarefa do Kaspersky Endpoint Security para um arquivo de texto

1. Na barra de menus, selecione **Proteção** > **Relatórios**.

   Será exibida a janela **Relatórios**.

2. No painel esquerdo, selecione uma guia com o relatório necessário.

3. No canto superior direito, clique em .

4. Na janela exibida, especifique o nome do arquivo, as marcas e a pasta de destino do relatório.

5. Clique em **Salvar**.

Por padrão, o Kaspersky Endpoint Security não registra eventos informativos nos relatórios. Você pode ativar o registro de eventos informativos.

Ativar o registro de eventos informativos nos relatórios

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Interface**, na seção **Relatórios**, marque a caixa de seleção **Registrar eventos não críticos** para receber notificações sobre eventos informativos do Kaspersky Endpoint Security.

Managed Detection and Response

O componente Managed Detection and Response foi adicionado ao Kaspersky Endpoint Security na versão 11.2. Esse componente interage com uma solução conhecida como Kaspersky Managed Detection and Response. O *Kaspersky Managed Detection and Response (MDR)* pesquisa, detecta e elimina continuamente ameaças direcionadas à sua organização. Para obter informações detalhadas sobre como a solução funciona, consulte a *ajuda do Kaspersky Managed Detection and Response*.

Ao interagir com o Kaspersky Managed Detection and Response, o aplicativo permite que você execute as seguintes funções:

- Ativar o Managed Detection and Response usando um arquivo de configuração BLOB.
- Executar comandos do Kaspersky Managed Detection and Response.
- Enviar dados de telemetria para o Kaspersky Managed Detection and Response para detecção de ameaças.

O componente Managed Detection and Response possui os seguintes requisitos adicionais:

- macOS 14 ou posterior
- Mac baseado em Intel, Apple Silicon
- Licença ativa do Kaspersky Endpoint Security

É necessário ativar os seguintes componentes para que o Managed Detection and Response funcione:

- Proteção Contra Ameaças ao Arquivo
- Proteção Contra Ameaças da Web
- Proteção Contra Ameaças ao Correio

A ativação desses componentes não é opcional. Caso contrário, o Kaspersky Managed Detection and Response não poderá funcionar porque não recebe os dados de telemetria necessários.

Além disso, o Kaspersky Managed Detection and Response usa dados recebidos de outros componentes do aplicativo. A ativação desses componentes é opcional. Os componentes que fornecem dados adicionais incluem:

- Detecção de Comportamento

Integração com o Kaspersky Managed Detection and Response

A integração com o Kaspersky Managed Detection and Response consiste nas seguintes etapas:

1. **Configurar o servidor proxy da Kaspersky Security Network**

   O servidor proxy da Kaspersky Security Network facilita a troca de dados entre computadores e a infraestrutura de serviço em nuvem da Kaspersky Security Network por meio do Servidor de Administração em vez da troca direta.

   Carregar o arquivo de configuração da Kaspersky Security Network nas propriedades do Servidor de Administração. O arquivo de configuração da Kaspersky Security Network está localizado no arquivo comprimido ZIP do arquivo de configuração do MDR. Você pode obter o arquivo comprimido ZIP no Kaspersky Managed Detection and Response Console. Para obter detalhes sobre como configurar o servidor proxy da Kaspersky Security Network, consulte a *ajuda do Kaspersky Security Center*.

   Como resultado, o Kaspersky Endpoint Security usará a KSN Privada para determinar a reputação de arquivos, aplicativos e sites. O status operacional da "*Infraestrutura: Kaspersky Private Security Network*" é indicado nas configurações de política na seção Kaspersky Security Network.

O uso da KSN Privada com o Kaspersky Managed Detection and Response garante que a telemetria seja enviada para servidores em conformidade com o GDPR (Regulamento Geral de Proteção de Dados). Se a KSN Privada não for usada, a telemetria poderá ser enviada para a KSN Global. Isso pode violar as leis de seu país.

Importante: você deve ativar o modo KSN estendido para que o Managed Detection and Response funcione.

2. **Ativação do Kaspersky Managed Detection and Response**

É possível ativar o componente Managed Detection and Response no dispositivo de endpoint por meio dos seguintes métodos:

- **Ativar com o uso de um código de ativação no aplicativo Kaspersky Endpoint Security**.

  1. Abra a janela principal do aplicativo.
  2. Na barra lateral da janela principal do aplicativo, clique em **Licença**.

     A janela **Licença** será exibida.
  3. Na janela **Licença**, digite o código de ativação recebido durante a compra.

     Nota: o código de ativação é uma combinação exclusiva de vinte letras latinas e números no formato xxxxx-xxxxx-xxxxx xxxxx.
  4. Clique em **Ativar**.

     O aplicativo se conecta aos servidores de ativação da Kaspersky e envia o código de ativação para verificar sua autenticidade. Se o código de ativação for verificado com êxito, o aplicativo receberá e adicionará automaticamente a chave de licença.

     Nota: dependendo do código de ativação que você recebeu, talvez seja necessário preencher um formulário de registro.

  Se a verificação do código falhar, será exibida uma notificação correspondente. Nesse caso, entre em contato com o fornecedor de software que forneceu esse código de ativação.

- **Ativar com o uso do arquivo BLOB**.

  Carregue o arquivo de configuração BLOB na política do Kaspersky Endpoint Security (veja as instruções abaixo). O arquivo BLOB contém o ID do cliente e informações sobre a licença do Kaspersky Managed Detection and Response. O arquivo BLOB está localizado no arquivo comprimido ZIP do arquivo de configuração do MDR. Você pode obter o arquivo comprimido ZIP no Kaspersky Managed Detection and Response Console. Para obter informações detalhadas sobre um arquivo BLOB, consulte a *ajuda do Kaspersky Managed Detection and Response*.

  Ative o Kaspersky Managed Detection and Response no Console de Administração (MMC)

  1. Inicie o Console de Administração do Kaspersky Security Center.
  2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
  3. Na árvore do console, clique em **Dispositivos gerenciados**.

4. Na área de trabalho, selecione a guia **Políticas**.

5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.

6. Na janela **Propriedades**, selecione **Detection and Response** > **Managed Detection and Response**.

7. Marque a caixa de seleção **Ativar Managed Detection and Response**.

8. No bloco **Arquivo de configuração do MDR**, clique em **Importar** e selecione o arquivo BLOB recebido no Kaspersky Managed Detection and Response Console. O arquivo tem a extensão .P7.

9. Clique em **OK** para salvar suas alterações.

Ative o Kaspersky Managed Detection and Response no Web Console e no Cloud Console

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

2. Clique no nome da política do Kaspersky Endpoint Security for Mac.

3. A janela de propriedades da política é aberta.

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

5. Selecione **Detection and Response** > **Managed Detection and Response**.

6. Ative o botão de alternância do **Managed Detection and Response**.

7. Clique **Importar** e selecione o arquivo BLOB obtido no Kaspersky Managed Detection and Response Console. O arquivo tem a extensão .P7.

8. Salve suas alterações.

Como resultado, o Kaspersky Endpoint Security verificará o arquivo BLOB. A verificação do arquivo BLOB inclui a verificação da assinatura digital e do termo da licença. Se o arquivo BLOB for verificado com êxito, o Kaspersky Endpoint Security carregará o arquivo e o enviará ao computador durante a próxima sincronização com o Kaspersky Security Center.

- **Ativar com o uso da tarefa Adicionar chave**.

  - **Ative o Kaspersky Managed Detection and Response no Console de Administração (MMC)**

    1. Na janela **Selecionar o tipo de tarefa**, maximize o nó do **Kaspersky Endpoint Security for Mac 12.2.1**.

    2. Para criar uma tarefa para adicionar uma chave, selecione **Adicionar chave**.

    3. Na janela **Ativação do aplicativo**, faça o seguinte:

       a. Selecione um código ou chave de ativação no armazenamento do Kaspersky Security Center ou adicione um arquivo de chave armazenado no seu computador.

       b. Para adicionar a chave especificada como chave reserva, marque a caixa de seleção **Adicionar uma chave reserva**.

          A chave reserva fica ativa quando a chave ativa atual expira.

As informações sobre a chave especificada (chave, tipo de chave e data de validade da chave) são exibidas na janela **Ativação do aplicativo**.

4. Na janela Selecionar os dispositivos aos quais a tarefa será atribuída, selecione o método que deseja usar para especificar computadores clientes:

   - Para selecionar entre os computadores detectados na rede pelo Servidor de Administração, selecione a opção **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**.

   - Para especificar os endereços IP dos computadores manualmente ou importar os endereços IP dos computadores de um arquivo, selecione a opção **Especificar os endereços do dispositivo manualmente ou importar os endereços da lista**.

   - Para criar uma tarefa para uma seleção de dispositivos com base em um critério predefinido, selecione a opção **Atribuir a tarefa a uma seleção de dispositivos**.

   - Para selecionar computadores de um grupo de administração específico, selecione a opção **Atribuir uma tarefa à um grupo de administração**.

5. Na janela que se abre (**Selecionar dispositivos**, **Seleção de dispositivos** ou **Selecionar grupo de Administração**, dependendo da opção selecionada na etapa anterior), selecione os computadores clientes, especifique os endereços IP dos computadores, especifique uma seleção de computadores ou selecione o grupo de administração ao qual a tarefa será aplicada.

   Nota: esta etapa não é relevante para tarefas locais ou de grupo.

6. Na janela **Configurar agendamento da tarefa**, selecione o modo de início na lista suspensa **Início agendado**.

7. Se necessário, configure uma tarefa agendada para iniciar automaticamente (especificando a data e hora de início da tarefa).

8. Se você deseja executar tarefas que o aplicativo não conseguiu iniciar de acordo com a programação (por exemplo, porque o computador foi desligado no horário agendado), marque a caixa de seleção **Executar tarefas ignoradas**.

   O Kaspersky Endpoint Security inicia a tarefa assim que o obstáculo que impede a inicialização da tarefa for eliminado.

9. Se desejar que o Kaspersky Security Center determine automaticamente o intervalo entre a inicialização da tarefa em computadores diferentes, marque a caixa de seleção **Usar atraso aleatório automaticamente para início das tarefas**.

   Isso ajuda a reduzir a carga no Servidor de Administração do Kaspersky Security Center.

10. Para definir manualmente o intervalo entre as inicializações de tarefas em computadores diferentes, marque a caixa de seleção **Usar atraso aleatório para inicialização de tarefas dentro de um intervalo de (min)** e especifique o número de minutos.

    Isso ajuda a reduzir a carga no Servidor de Administração do Kaspersky Security Center.

11. Na janela **Definir o nome da tarefa**, digite o nome da tarefa que você está criando no campo **Nome**.

1. Na janela **Concluir a criação da tarefa**, faça o seguinte:

a. Se desejar que a tarefa seja iniciada assim que o assistente for concluído, marque a caixa de seleção **Executar tarefa após finalizar o Assistente**.

b. Clique em **Finalizar** para fechar o assistente.

- **Ative o Kaspersky Managed Detection and Response no Web Console e no Cloud Console**

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** > **Tarefas**.

   A lista de tarefas é aberta.

2. Clique em **Adicionar**.

   O **Assistente para novas tarefas** é iniciado.

3. Definir os ajustes da tarefa:

   a. Na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Mac (12.2.1).

   b. Na lista suspensa **Tipo de tarefa**, selecione **Adicionar chave**.

   c. No campo **Nome da tarefa**, insira uma breve descrição.

   d. Selecione uma das seguintes opções:

   - **Atribuir tarefa a um grupo de administração**

     A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo.

     Por exemplo, você pode querer usar esta opção para executar uma tarefa de enviar uma mensagem aos usuários se a mensagem for específica para dispositivos incluídos em um grupo de administração específico.

     Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas aos ajustes de segurança dos grupos aos quais se aplicam.

   - **Especificar endereços de dispositivo manualmente ou importar endereços de uma lista**

     Você pode especificar nomes NetBIOS, nomes DNS, endereços IP e sub-redes IP de dispositivos aos quais deseja atribuir a tarefa.

     Você pode usar esta opção para executar uma tarefa para uma sub-rede específica. Por exemplo, convém instalar um determinado aplicativo em dispositivos de contadores ou verificar dispositivos em uma sub-rede que provavelmente está infectada.

   - **Atribuir tarefa a uma seleção de dispositivo**

     A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar um das opções existentes:

     Por exemplo, você pode usar esta opção para executar uma tarefa em dispositivos com uma versão específica do sistema operacional.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada.

5. Selecione a chave de licença na lista. Caso a lista não contenha uma licença apropriada, será possível adicionar uma nova chave de licença ao repositório do Servidor de Administração.

6. Insira as credenciais da conta do usuário cujos direitos você deseja usar para executar a tarefa. Clique em **Avançar**.

   Nota: Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (raiz).

7. Na etapa **Concluir a criação da tarefa**, clique no botão **Concluir** para criar a tarefa e fechar o assistente.

   Se você ativou a opção **Abrir detalhes da tarefa quando a criação estiver concluída**, a janela de ajustes da tarefa é aberta. Nessa janela, você pode verificar os parâmetros da tarefa, modificá-los ou configurar um agendamento de início de tarefa, se necessário.

8. Clique na nova tarefa.

   A janela de propriedades da tarefa é aberta.

9. Selecione a guia **Agendamento**.

10. Configure o agendamento de tarefas.

    Nota: Assegure-se de que o computador esteja ligado para executar a tarefa.

11. Clique em **Salvar**.

12. Para executar a tarefa imediatamente, independentemente do agendamento configurado, faça o seguinte:

    a. Marque a caixa de seleção ao lado da tarefa.

    b. Clique no botão **Executar**.

Endpoint Detection and Response Expert (on-premise)

O Kaspersky Endpoint Security é compatível com a integração do componente Kaspersky Endpoint Detection and Response como parte da solução Kaspersky Anti Targeted Attack Platform. Esta solução foi desenvolvida para detectar prontamente as ameaças avançadas, como ataques direcionados, ameaças persistentes avançadas, ataques de dia zero e outros. Para obter informações detalhadas sobre como a solução funciona, consulte a *ajuda do Kaspersky Anti Targeted Attack Platform*.

Quando a integração com o Endpoint Detection and Response (KATA) é configurada, o servidor KATA recebe informações sobre os eventos que ocorrem na operação do Kaspersky Endpoint Security, ameaças descobertas pelo aplicativo, além das informações sobre o modo pelo qual o processamento dessas ameaças. Para reagir às ameaças detectadas, o Kaspersky Endpoint Security pode executar tarefas iniciadas na interface da Web do Kaspersky Anti Targeted Attack Platform.

O Endpoint Detection and Response Expert (on-premise) possui os seguintes requisitos adicionais:

- Kaspersky Anti Targeted Attack Platform 6.0 ou posterior.
- A versão do Kaspersky Security Center é a 14.2 ou superior.
- A integração com o Endpoint Detection and Response Expert (versão 7.1 ou anterior) pode ser configurada no Console de Administração do Kaspersky Security Center (MMC), no Web Console ou no Cloud Console.
- A integração com o Endpoint Detection and Response Expert (versão 8.0 ou posterior) pode ser configurada no Console de Administração do Kaspersky Security Center (MMC), no Web Console ou no Cloud Console.

Integração com o Kaspersky Endpoint Detection and Response (KATA)

A integração com o Kaspersky Endpoint Detection and Response (KATA) consiste nas seguintes etapas:

1. **Instalar o componente Endpoint Detection and Response**

   É possível selecionar o componente Endpoint Detection and Response durante a instalação do Kaspersky Endpoint Security.

2. **Ativar o Endpoint Detection and Response**

   Caso o componente Endpoint Detection and Response não seja compatível com sua licença atual, será necessário ativar separadamente o Kaspersky Endpoint Detection and Response.

   É possível verificar se a funcionalidade Endpoint Detection and Response é compatível com a licença atual na janela **Licença**.

3. **Conectar a um servidor KATA**

   O Kaspersky Anti Targeted Attack Platform requer o estabelecimento de uma conexão confiável entre o Kaspersky Endpoint Security e um servidor KATA. Para configurar uma conexão confiável, é necessário usar um certificado TLS. É possível baixar um certificado TLS na interface da Web do Kaspersky Anti Targeted Attack Platform. Para obter informações detalhadas sobre como baixar um certificado, consulte a *ajuda do Kaspersky Anti Targeted Attack Platform*.

   Por padrão, o Kaspersky Endpoint Security verifica somente o certificado TLS do servidor KATA. Para tornar a conexão mais segura, é possível ativar a verificação bidirecional. Para usar a verificação bidirecional, será necessário usar um contêiner de criptografia protegido por senha. Para obter informações detalhadas sobre o download de um contêiner de criptografia, consulte a *ajuda do Kaspersky Anti Targeted Attack Platform*.

   Conecte computadores com o Kaspersky Endpoint Security a um servidor KATA com o uso do Console de Administração

   1. Inicie o Console de Administração.
   2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
   3. Na árvore do console, clique em **Dispositivos gerenciados**.
   4. Na área de trabalho, selecione a guia **Políticas**.
   5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
   6. Na janela **Propriedades**, selecione **Detection and Response** > **Endpoint Detection and Response Expert (on-premise)**.

7. Marque a caixa de seleção **Ativar o Endpoint Detection and Response Expert (versão 7.1 ou anterior)**.

8. Clique em **Configurações de conexão do servidor**.

9. Na janela exibida **Configurações de conexão do servidor**, defina as seguintes configurações:

    - Clique em **Carregar certificado TLS** para selecionar um certificado TLS que será usado para estabelecer uma conexão confiável com um servidor KATA.

    - Caso queira alterar o tempo limite de resposta do servidor KATA, especifique o tempo limite no campo **Tempo esgotado (s)**. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta se conectar a um servidor KATA diferente.

    - Caso queira usar a verificação bidirecional, marque a caixa de seleção **Usar autenticação em duas etapas**. Clique em **Carregar contêiner de criptografia** para selecionar um arquivo de contêiner de criptografia e insira a senha no campo **Senha do contêiner de criptografia**.

10. Clique em **Salvar**.

11. Para adicionar um servidor KATA, clique em **Adicionar**.

12. Na janela aberta do **Servidor KATA**, especifique o endereço, a porta do servidor e clique em **Salvar**.

13. Clique em **OK** para salvar suas alterações.

Conecte os computadores com o Kaspersky Endpoint Security com um servidor KATA usando o Web Console

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

2. Clique no nome da política do Kaspersky Endpoint Security for Mac.

    A janela de propriedades da política é aberta.

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

4. Selecione **Detection and Response** > **Endpoint Detection and Response Expert (on-premise)**.

5. Ative o botão de alternância do **Endpoint Detection and Response Expert (on-premise)**.

6. Clique em **Configurações de conexão**.

7. Na janela exibida **Configurações de conexão do servidor**, defina as seguintes configurações:

    - Clique em **Adicionar certificado TLS** para selecionar um certificado TLS que será usado para estabelecer uma conexão confiável com um servidor KATA.

    - Caso queira alterar o tempo limite de resposta do servidor KATA, especifique o tempo limite no campo **Tempo esgotado (s)**. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta se conectar a um servidor KATA diferente.

    - Caso queira usar a verificação bidirecional, marque a caixa de seleção **Usar autenticação de duas etapas**. Clique em **Carregar contêiner de criptografia** para selecionar um arquivo de contêiner de criptografia e insira a senha no campo **Senha do contêiner de criptografia**.

8. Clique em **OK**.

9. Para adicionar um servidor KATA, clique em **Adicionar**.
10. Na caixa de diálogo exibida, especifique o endereço do servidor, a porta e clique em **OK**.
11. Salve suas alterações.

Depois disso, os computadores serão exibidos na interface da Web do Kaspersky Anti Targeted Attack Platform.

Endpoint Detection and Response Optimum

A partir da versão 12.1, o Kaspersky Endpoint Security for Mac inclui um agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum (doravante também "EDR Optimum"). Essa solução foi projetada para proteger a infraestrutura de TI corporativa contra ameaças cibernéticas avançadas. A funcionalidade da solução combina a detecção automática de ameaças com a capacidade de reagir a essas ameaças para neutralizar ataques avançados, incluindo novos exploits, ransomwares, ataques sem arquivo, bem como métodos que usam ferramentas de sistema legítimas. Para obter detalhes sobre a solução, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum.

O Kaspersky Endpoint Detection and Response revisa e analisa o desenvolvimento de ameaças e fornece à *equipe de segurança* ou ao *Administrador* as informações sobre o possível ataque necessárias para uma resposta oportuna. O Kaspersky Endpoint Detection and Response exibe os detalhes de alertas e uma janela separada. *Detalhes do alerta* é uma ferramenta para exibir a totalidade das informações coletadas sobre uma ameaça detectada. Os detalhes do alerta incluem, por exemplo, o histórico de arquivos que aparecem no computador. Para obter detalhes sobre o gerenciamento de detalhes do alerta, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum.

Nota: você pode configurar o componente EDR Optimum no Web Console.

Configurações do Endpoint Detection and Response

Parâmetro	Descrição
Isolamento de rede	Isolamento automático do computador da rede em resposta a ameaças detectadas. Quando o isolamento de rede está ativado, o aplicativo corta todas as conexões ativas e bloqueia todas as novas conexões TCP/IP no computador. O aplicativo deixa apenas as seguintes conexões ativas: • Conexões listadas em Exclusões de isolamento de rede. • Conexões iniciadas pelos serviços do Kaspersky Endpoint Security. • Conexões iniciadas pelo Agente de Rede do Kaspersky Security Center.
Desbloquear automaticamente o computador isolado em N horas	O isolamento de rede pode ser desativado automaticamente após um tempo especificado ou manualmente. Por padrão, o Kaspersky Endpoint Security desativa o isolamento de rede 8 horas após o início do isolamento.
Exclusões de isolamento de rede	Lista de regras para exclusões do isolamento de rede. As conexões de rede que correspondem às regras não são bloqueadas nos computadores quando o isolamento de rede está ativado. Para configurar as exclusões de isolamento de rede, você pode usar uma lista de perfis de rede padrão. Por padrão, as exclusões incluem perfis de rede que contêm regras que garantem a operação ininterrupta de dispositivos com as funções de servidor DNS/DHCP e cliente DNS/DHCP. Você também pode modificar os ajustes de perfis de rede padrão ou definir as exclusões manualmente. **Importante:** as exclusões especificadas nas propriedades da política são aplicadas somente se o isolamento de rede for ativado automaticamente em resposta a uma ameaça detectada. As exclusões especificadas nas propriedades do computador são aplicadas somente se o Isolamento de rede estiver ativado manualmente nas propriedades do computador no console do Kaspersky Security Center ou nos detalhes do alerta.

Parâmetro	Descrição
Prevenção de execução	A prevenção de execução permite gerenciar a execução de arquivos executáveis e scripts, assim como abrir arquivos no formato do Office. Dessa forma, você pode, por exemplo, impedir a execução de aplicativos que considera inseguros. Como resultado, a disseminação da ameaça pode ser interrompida. A prevenção de execução dá suporte a um conjunto de interpretadores de script. Para usar o componente Prevenção de execução, você precisa adicionar regras de prevenção de execução. A regra de prevenção de execução é um conjunto de critérios que o aplicativo leva em consideração ao reagir à execução de um objeto, por exemplo, ao bloquear a execução do objeto. O aplicativo identifica arquivos por seus caminhos ou somas de verificação calculadas usando algoritmos de hash MD5 e SHA256.
Ação na execução ou abertura de objeto proibido	**Bloquear e gravar no relatório**. Nesse modo, o aplicativo bloqueia a execução de objetos ou a abertura de documentos que atendem aos critérios da regra de prevenção. O aplicativo também publica um evento sobre tentativas de executar objetos ou abrir documentos no log de eventos do Kaspersky Security Center e no sistema de login unificado. **Criar log de eventos apenas**. Nesse modo, o Kaspersky Endpoint Security publica um evento sobre tentativas de executar objetos executáveis ou documentos abertos que correspondem aos critérios da regra de prevenção no log de eventos do Kaspersky Security Center e no sistema de login unificado, mas não bloqueia a tentativa de executar ou abrir o objeto ou documento. Este modo está marcado por padrão.
Cloud Sandbox	O Cloud Sandbox é uma tecnologia que permite detectar ameaças avançadas em um computador. O Kaspersky Endpoint Security encaminha automaticamente arquivos detectados para a Cloud Sandbox analisar. O Cloud Sandbox executa esses arquivos em um ambiente isolado para identificar atividades maliciosas e avaliar a sua reputação. Os dados nesses arquivos são então enviados para a Kaspersky Security Network. Portanto, caso o Cloud Sandbox detecte um arquivo malicioso, o Kaspersky Endpoint Security executará a ação apropriada para eliminar essa ameaça em todos os computadores em que esse arquivo for detectado. **Nota:** A tecnologia Cloud Sandbox é permanentemente ativada e está disponível para todos os usuários da Kaspersky Security Network, independentemente do tipo de licença que estão usando.

Integração com o Endpoint Detection and Response Optimum

Para integrar com o Kaspersky Endpoint Detection and Response, você deve adicionar o componente Endpoint Detection and Response Optimum (EDR Optimum) e configurar o Kaspersky Endpoint Security.

Nota: Os componentes EDR Optimum e Endpoint Detection and Response (KATA) não são compatíveis entre si.

As seguintes condições devem ser atendidas para que o Endpoint Detection and Response funcione:

- A versão do Kaspersky Security Center é a 13.2 ou superior. Em versões anteriores do Kaspersky Security Center, é impossível ativar o recurso Endpoint Detection and Response.
- O plugin de administração do Kaspersky Endpoint Detection and Response está instalado. Este é um plugin único para trabalhar com agentes em sistemas operacionais Windows, Mac e Linux. Ao trabalhar com o Endpoint Detection and Response Optimum, você precisará do plugin de administração do Kaspersky Endpoint Security para criar tarefas de resposta a ameaças e do plugin de administração do EDR para visualizar detalhes de alertas.
- O componente EDR Optimum como parte do Kaspersky Endpoint Security é compatível com a interação da solução Kaspersky Endpoint Detection and Response Optimum 3.0. A interação com versões anteriores do Kaspersky Endpoint Detection and Response Optimum não é compatível.
- O EDR Optimum pode ser gerenciado no Web Console.

- O aplicativo é ativado e a funcionalidade é coberta pela licença.
- O componente Endpoint Detection and Response está ativado.

Integração com o Kaspersky Endpoint Detection and Response Optimum

A integração com o Kaspersky Endpoint Detection and Response Optimum consiste nas seguintes etapas:

1. **Instalar o componente Endpoint Detection and Response Optimum**

   É possível selecionar o componente Endpoint Detection and Response durante a instalação do Kaspersky Endpoint Security.

2. **Ativar o Endpoint Detection and Response**

   Caso o componente Endpoint Detection and Response não seja compatível com sua licença atual, será necessário ativar separadamente o Kaspersky Endpoint Detection and Response.

   É possível verificar se a funcionalidade Endpoint Detection and Response é compatível com a licença atual na janela **Licença**.

3. **Ativar o componente Endpoint Detection and Response**

   Você pode ativar ou desativar o componente nos ajustes da política do Kaspersky Endpoint Security for Mac.

   Como ativar ou desativar o componente Endpoint Detection and Response no Web Console

   1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
   2. Clique no nome da política do Kaspersky Endpoint Security.

      A janela de propriedades da política é aberta.
   3. Selecione a guia **Configurações do aplicativo**.
   4. Vá para **Detection and Response** > **Endpoint Detection and Response**.
   5. Ative o botão de alternância do **Endpoint Detection and Response Expert (on-premise)**.
   6. Salve suas alterações.

Verificar indicadores de comprometimento

Um **Indicador de Comprometimento (IOC)** é um conjunto de dados sobre um objeto ou atividade que indica acesso não autorizado ao computador (comprometimento de dados). Por exemplo, muitas tentativas malsucedidas de entrar no sistema podem constituir um indicador de comprometimento. A tarefa **Verificação de IOC** permite encontrar Indicadores de comprometimento no computador e tomar medidas de resposta a ameaças.

O Kaspersky Endpoint Security procura indicadores de comprometimento usando arquivos IOC. Os arquivos IOC são arquivos que contêm os conjuntos de indicadores que o aplicativo tenta corresponder para contar uma detecção. Os arquivos IOC devem estar em conformidade com os requisitos para arquivos IOC.

Modo de execução da tarefa de Verificação IOC

O Kaspersky Endpoint Detection and Response permite criar tarefas padrão de verificação de IOC para detectar dados comprometidos. A tarefa de verificação IOC padrão é um grupo ou tarefa local criada e configurada manualmente no Web Console. As tarefas são executadas usando arquivos IOC preparados pelo usuário. Se você quiser adicionar um indicador de comprometimento manualmente, leia os requisitos para arquivos IOC.

Criar uma tarefa de Verificação de IOC

Você pode criar tarefas de Verificação de IOC manualmente:

- Nos detalhes do alerta (somente para EDR Optimum).

  Detalhes do alerta é uma ferramenta para exibir a totalidade das informações coletadas sobre uma ameaça detectada. Os detalhes do alerta incluem, por exemplo, o histórico de arquivos que aparecem no computador. Para obter detalhes sobre o gerenciamento de detalhes do alerta, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum.

- Usando o Assistente de Tarefas.

Para criar uma tarefa de Verificação de IOC:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** > **Tarefas**.

   A lista de tarefas é aberta.

2. Clique em **Adicionar**.

   O **Assistente para novas tarefas** é iniciado.

3. Definir os ajustes da tarefa:

   a. Na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Mac (12.2.1).

   b. Na lista suspensa **Tipo de tarefa**, selecione **Verificação de IOC**.

   c. No campo **Nome da tarefa**, insira uma breve descrição.

   d. No bloco **Selecionar dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada.

5. Na seção **Ajustes da verificação de IOC**, carregue os arquivos IOC para procurar indicadores de comprometimento. É possível adicionar um arquivo IOC ou gerar um a partir de um arquivo com hashes de arquivos ou endereços IP.

   Depois de carregar os arquivos IOC, é possível visualizar e editar a lista de indicadores dos arquivos IOC.

   Nota: não é recomendado adicionar ou remover arquivos IOC depois de executar a tarefa. Isso pode fazer com que os resultados da verificação de IOC sejam exibidos incorretamente para execuções anteriores da tarefa. Para pesquisar indicadores de comprometimento por novos arquivos IOC, recomenda-se adicionar novas tarefas.

6. Configurar ações ao detectar IOC:

   - **Isolar o computador da rede**. Caso a opção seja selecionada, o Kaspersky Endpoint Security isola o computador da rede para evitar que a ameaça se espalhe. É possível configurar a duração do isolamento no componente de configurações do Endpoint Detection and Response.

   - **Mover cópia para a Quarentena e excluir objeto**. Caso a opção seja selecionada, o Kaspersky Endpoint Security exclui o objeto malicioso encontrado no computador. Antes de excluir o objeto, o Kaspersky Endpoint Security cria uma cópia de backup, caso o objeto precise ser restaurado posteriormente. O Kaspersky Endpoint Security move a cópia de backup para a quarentena.

   - **Executar verificação de áreas críticas**. Se esta opção estiver selecionada, o Kaspersky Endpoint Security executa a tarefa de Verificação Rápida. Por padrão, o Kaspersky Endpoint Security verifica a memória, os objetos de inicialização e as pastas do sistema.

7. Vá para a seção **Avançado**.

8. Selecione os tipos de dados (documentos IOC) que devem ser analisados como parte da tarefa.

   Nota: O Kaspersky Endpoint Security seleciona automaticamente os tipos de dados (documentos IOC) para a tarefa de Verificação IOC de acordo com o conteúdo dos arquivos IOC carregados. Não é recomendável desmarcar os tipos de dados.

   Você também pode configurar escopos da verificação para os seguintes tipos de dados:

   - **Processos - ProcessItem**
   - **Arquivos – FileItem**
   - **Portas de rede – PortItem**
   - **Contas de usuários - UserItem**
   - **Tabelas ARP - ArpEntryItem**
   - **Hosts - SystemInfoItem**
   - **URLs – UrlHistoryItem**
   - **Rotas – RouteEntryItem**

9. Clique em **OK**.

10. Insira as credenciais da conta do usuário cujos direitos você deseja usar para executar a tarefa. Clique em **Avançar**.

    Nota: Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (raiz).

11. Na etapa **Concluir a criação da tarefa**, clique no botão **Concluir** para criar a tarefa e fechar o assistente.

    Se você ativou a opção **Abrir detalhes da tarefa quando a criação estiver concluída**, a janela de ajustes da tarefa é aberta. Nessa janela, você pode verificar os parâmetros da tarefa, modificá-los ou configurar um agendamento de início de tarefa, se necessário.

12. Clique na nova tarefa.

    A janela de propriedades da tarefa é aberta.

13. Selecione a guia **Agendamento**.

14. Configure o agendamento de tarefas.

    Nota: Assegure-se de que o computador esteja ligado para executar a tarefa.

15. Clique em **Salvar**.

16. Para executar a tarefa imediatamente, independentemente do agendamento configurado, faça o seguinte:

    a. Marque a caixa de seleção ao lado da tarefa.

    b. Clique no botão **Executar**.

17. Como resultado, o Kaspersky Endpoint Security executa a pesquisa de indicadores de comprometimento do computador. Você pode exibir os resultados da tarefa nas propriedades da tarefa na seção **Resultados**. Você pode exibir as informações sobre os indicadores de comprometimento detectados nas propriedades da tarefa: **Ajustes do aplicativo** > **Resultados da verificação de IOC**.

Nota: os resultados da verificação de IOC são mantidos por 30 dias. Após esse período, o Kaspersky Endpoint Security exclui as entradas mais antigas automaticamente.

Mover arquivo para a Quarentena

Ao reagir a ameaças, o Kaspersky Endpoint Detection and Response pode criar tarefas *Mover arquivo para a Quarentena*. Isso é necessário para minimizar as consequências da ameaça. A *Quarentena* é um armazenamento local especial no computador. O usuário pode colocar em quarentena arquivos que considerar perigosos para o computador. Os arquivos de quarentena são armazenados em um estado criptografado e não ameaçam a segurança do dispositivo. O Kaspersky Endpoint Security usa o Backup como um armazenamento de arquivos. Para obter detalhes sobre o gerenciamento da Quarentena como parte das soluções, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum.

Você pode criar tarefas *Mover arquivo para a Quarentena* das seguintes formas:

- Nos detalhes do alerta (somente para EDR Optimum).

  Detalhes do alerta é uma ferramenta para exibir a totalidade das informações coletadas sobre uma ameaça detectada. Os detalhes do alerta incluem, por exemplo, o histórico de arquivos que aparecem no computador. Para obter detalhes sobre o gerenciamento de detalhes do alerta, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum.

- Usando o Assistente de Tarefas.

  Você deve inserir o caminho do arquivo ou o hash (SHA256 ou MD5), ou ambos, o caminho do arquivo e o hash do arquivo.

A tarefa *Mover arquivo para a Quarentena* tem as seguintes limitações:

- O tamanho do arquivo não deve exceder 100 MB.
- Você pode configurar a tarefa para EDR Optimum no Web Console.
- A capacidade do Backup é limitada pelo espaço livre em disco.

Para criar uma tarefa Mover arquivo para a Quarentena:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** > **Tarefas**.

   A lista de tarefas é aberta.

2. Clique em **Adicionar**.

   O **Assistente para novas tarefas** é iniciado.

3. Definir os ajustes da tarefa:

   a. Na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Mac (12.2.1).

   b. Na lista suspensa **Tipo de tarefa**, selecione **Mover arquivo para a Quarentena**.

   c. No campo **Nome da tarefa**, insira uma breve descrição.

   d. Selecione uma das seguintes opções:

   - **Atribuir tarefa a um grupo de administração**

     A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo.

     Por exemplo, você pode querer usar esta opção para executar uma tarefa de enviar uma mensagem aos usuários se a mensagem for específica para dispositivos incluídos em um grupo de administração específico.

     Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas aos ajustes de segurança dos grupos aos quais se aplicam.

   - **Especificar endereços de dispositivo manualmente ou importar endereços de uma lista**

     Você pode especificar nomes NetBIOS, nomes DNS, endereços IP e sub-redes IP de dispositivos aos quais deseja atribuir a tarefa.

     Você pode usar esta opção para executar uma tarefa para uma sub-rede específica. Por exemplo, convém instalar um determinado aplicativo em dispositivos de contadores ou verificar dispositivos em uma sub-rede que provavelmente está infectada.

   - **Atribuir tarefa a uma seleção de dispositivo**

     A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar um das opções existentes:

     Por exemplo, você pode usar esta opção para executar uma tarefa em dispositivos com uma versão específica do sistema operacional.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada.

5. Na etapa **Escopo da tarefa**, especifique um grupo de administração, dispositivos com endereços específicos ou uma seleção de dispositivos.

   Os ajustes disponíveis dependem da opção selecionada na etapa anterior.

6. Na lista de arquivos, clique em **Adicionar**.

   O assistente de adição de arquivo é iniciado.

7. Na lista suspensa **Especifique o arquivo a ser movido na Quarentena**, selecione uma das opções e preencha os campos necessários. Para adicionar o arquivo, você deve inserir o caminho completo para o arquivo ou o hash do arquivo e o caminho.

8. Se você quiser que seja possível aplicar a tarefa a objetos críticos do sistema, marque a caixa de seleção **Aplicar aos objetos críticos do sistema**.

9. Insira as credenciais da conta do usuário cujos direitos você deseja usar para executar a tarefa. Clique em **Avançar**.

   Nota: Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (raiz).

10. Na etapa **Concluir a criação da tarefa**, clique no botão **Concluir** para criar a tarefa e fechar o assistente.

    Se você ativou a opção **Abrir detalhes da tarefa quando a criação estiver concluída**, a janela de ajustes da tarefa é aberta. Nessa janela, você pode verificar os parâmetros da tarefa, modificá-los ou configurar um agendamento de início de tarefa, se necessário.

11. Clique na nova tarefa.

    A janela de propriedades da tarefa é aberta.

12. Selecione a guia **Agendamento**.

13. Configure o agendamento de tarefas.

    Nota: Assegure-se de que o computador esteja ligado para executar a tarefa.

14. Clique em **Salvar**.

15. Para executar a tarefa imediatamente, independentemente do agendamento configurado, faça o seguinte:

    a. Marque a caixa de seleção ao lado da tarefa.

    b. Clique no botão **Executar**.

Como resultado, o Kaspersky Endpoint Security move o arquivo para a quarentena.

A tarefa *Mover arquivo para a Quarentena* pode ser concluída com o erro *Acesso negado* se você estiver tentando colocar em quarentena um arquivo executável em execução no momento. Crie uma tarefa de encerramento do processo para o arquivo e tente novamente.

A tarefa *Mover arquivo para a Quarentena* pode ser concluída com o erro *Espaço insuficiente no armazenamento da Quarentena* se você estiver tentando colocar em quarentena um arquivo muito grande. Libere espaço no disco e tente novamente.

Obter arquivo

Você pode obter arquivos de computadores de usuários. Por exemplo, você pode configurar a obtenção de um arquivo de log de eventos criado por um aplicativo de terceiros. Para obter o arquivo, você deve criar uma tarefa dedicada. Como resultado da execução da tarefa, o arquivo é salvo no Backup. Você pode baixar esse arquivo do Backup para o computador usando o Web Console. No computador do usuário, o arquivo permanece em sua pasta original.

Importante: o tamanho do arquivo não deve exceder 100 MB. A capacidade do Backup é limitada pelo espaço livre em disco.

Para criar uma tarefa Obter arquivo:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** > **Tarefas**.

   A lista de tarefas é aberta.

2. Clique em **Adicionar**.

   O **Assistente para novas tarefas** é iniciado.

3. Definir os ajustes da tarefa:

   a. Na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Mac (12.2.1).

   b. Na lista suspensa **Tipo de tarefa**, selecione **Obter arquivo**.

   c. No campo **Nome da tarefa**, insira uma breve descrição.

   d. Selecione uma das seguintes opções:

   - **Atribuir tarefa a um grupo de administração**

     A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo.

     Por exemplo, você pode querer usar esta opção para executar uma tarefa de enviar uma mensagem aos usuários se a mensagem for específica para dispositivos incluídos em um grupo de administração específico.

     Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas aos ajustes de segurança dos grupos aos quais se aplicam.

   - **Especificar endereços de dispositivo manualmente ou importar endereços de uma lista**

     Você pode especificar nomes NetBIOS, nomes DNS, endereços IP e sub-redes IP de dispositivos aos quais deseja atribuir a tarefa.

Você pode usar esta opção para executar uma tarefa para uma sub-rede específica. Por exemplo, convém instalar um determinado aplicativo em dispositivos de contadores ou verificar dispositivos em uma sub-rede que provavelmente está infectada.

- **Atribuir tarefa a uma seleção de dispositivo**

  A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar um das opções existentes:

  Por exemplo, você pode usar esta opção para executar uma tarefa em dispositivos com uma versão específica do sistema operacional.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Na janela **Obter o arquivo**, clique em **Adicionar**.

   A caixa de diálogo **Obter o arquivo** é aberta.

5. Na lista suspensa **Especifique qual arquivo você quer obter**, selecione uma das opções e preencha os campos obrigatórios.

   Para adicionar o arquivo, você deve inserir o caminho completo para o arquivo ou o hash do arquivo e o caminho.

6. Clique em **OK**.

   Os ajustes do arquivo a ser adicionado serão exibidos na lista de arquivos.

7. Clique em **Avançar**.

8. Insira as credenciais da conta do usuário cujos direitos você deseja usar para executar a tarefa. Clique em **Avançar**.

   Nota: Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (raiz).

9. Na etapa **Concluir a criação da tarefa**, clique no botão **Concluir** para criar a tarefa e fechar o assistente.

   Se você ativou a opção **Abrir detalhes da tarefa quando a criação estiver concluída**, a janela de ajustes da tarefa é aberta. Nessa janela, você pode verificar os parâmetros da tarefa, modificá-los ou configurar um agendamento de início de tarefa, se necessário.

10. Clique na nova tarefa.

    A janela de propriedades da tarefa é aberta.

11. Selecione a guia **Agendamento**.

12. Configure o agendamento de tarefas.

    Nota: Assegure-se de que o computador esteja ligado para executar a tarefa.

13. Clique em **Salvar**.

14. Para executar a tarefa imediatamente, independentemente do agendamento configurado, faça o seguinte:

    a. Marque a caixa de seleção ao lado da tarefa.

    b. Clique no botão **Executar**.

Como resultado, o Kaspersky Endpoint Security cria uma cópia do arquivo e move essa cópia para o Backup. Você pode baixar o arquivo do Backup no Web Console.

Excluir arquivo

Você pode excluir arquivos remotamente usando a tarefa *Excluir arquivo*. Por exemplo, você pode excluir remotamente um arquivo ao responder a ameaças.

Para criar uma tarefa Excluir arquivo:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** > **Tarefas**.

   A lista de tarefas é aberta.

2. Clique em **Adicionar**.

   O **Assistente para novas tarefas** é iniciado.

3. Definir os ajustes da tarefa:

    a. Na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Mac (12.2.1).

    b. Na lista suspensa **Tipo de tarefa**, selecione **Excluir arquivo**.

    c. No campo **Nome da tarefa**, insira uma breve descrição.

    d. Selecione uma das seguintes opções:

    - **Atribuir tarefa a um grupo de administração**

      A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo.

      Por exemplo, você pode querer usar esta opção para executar uma tarefa de enviar uma mensagem aos usuários se a mensagem for específica para dispositivos incluídos em um grupo de administração específico.

      Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas aos ajustes de segurança dos grupos aos quais se aplicam.

    - **Especificar endereços de dispositivo manualmente ou importar endereços de uma lista**

      Você pode especificar nomes NetBIOS, nomes DNS, endereços IP e sub-redes IP de dispositivos aos quais deseja atribuir a tarefa.

      Você pode usar esta opção para executar uma tarefa para uma sub-rede específica. Por exemplo, convém instalar um determinado aplicativo em dispositivos de contadores ou verificar dispositivos em uma sub-rede que provavelmente está infectada.

- **Atribuir tarefa a uma seleção de dispositivo**

  A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar um das opções existentes:

  Por exemplo, você pode usar esta opção para executar uma tarefa em dispositivos com uma versão específica do sistema operacional.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada.

5. Na lista suspensa **Especifique qual arquivo você quer excluir**, selecione uma das opções e preencha os campos necessários. Para adicionar o arquivo, você deve inserir o caminho completo para o arquivo ou o hash do arquivo e o caminho.

6. Se você quiser que seja possível aplicar a tarefa a objetos críticos do sistema, marque a caixa de seleção **Aplicar aos objetos críticos do sistema**.

7. Insira as credenciais da conta do usuário cujos direitos você deseja usar para executar a tarefa. Clique em **Avançar**.

   Nota: Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (raiz).

8. Na etapa **Concluir a criação da tarefa**, clique no botão **Concluir** para criar a tarefa e fechar o assistente.

   Se você ativou a opção **Abrir detalhes da tarefa quando a criação estiver concluída**, a janela de ajustes da tarefa é aberta. Nessa janela, você pode verificar os parâmetros da tarefa, modificá-los ou configurar um agendamento de início de tarefa, se necessário.

9. Clique na nova tarefa.

   A janela de propriedades da tarefa é aberta.

10. Selecione a guia **Agendamento**.

11. Configure o agendamento de tarefas.

    Nota: Assegure-se de que o computador esteja ligado para executar a tarefa.

12. Clique em **Salvar**.

13. Para executar a tarefa imediatamente, independentemente do agendamento configurado, faça o seguinte:

    a. Marque a caixa de seleção ao lado da tarefa.

    b. Clique no botão **Executar**.

Como resultado, o Kaspersky Endpoint Security exclui o arquivo do computador. Se o arquivo estiver bloqueado por um processo diferente, a tarefa será exibida como *Concluída*, mas o arquivo em si será excluído somente depois que o computador for reiniciado. Depois de reiniciar o computador, confirme se o arquivo foi excluído.

A tarefa *Excluir arquivo* pode ser concluída com o erro *Acesso negado* se você estiver tentando excluir um arquivo executável em execução no momento. Crie uma tarefa de encerramento do processo para o arquivo e tente novamente.

Iniciar processo

Você pode executar arquivos remotamente usando a tarefa *Iniciar processo*.

Importante: você pode configurar a tarefa para EDR Optimum no Web Console.

Para criar uma tarefa Iniciar processo:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** > **Tarefas**.

   A lista de tarefas é aberta.

2. Clique em **Adicionar**.

   O **Assistente para novas tarefas** é iniciado.

3. Definir os ajustes da tarefa:

   a. Na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Mac (12.2.1).

   b. Na lista suspensa **Tipo de tarefa**, selecione **Iniciar processo**.

   c. No campo **Nome da tarefa**, insira uma breve descrição.

   d. Selecione uma das seguintes opções:

   - **Atribuir tarefa a um grupo de administração**

     A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo.

     Por exemplo, você pode querer usar esta opção para executar uma tarefa de enviar uma mensagem aos usuários se a mensagem for específica para dispositivos incluídos em um grupo de administração específico.

     Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas aos ajustes de segurança dos grupos aos quais se aplicam.

   - **Especificar endereços de dispositivo manualmente ou importar endereços de uma lista**

     Você pode especificar nomes NetBIOS, nomes DNS, endereços IP e sub-redes IP de dispositivos aos quais deseja atribuir a tarefa.

     Você pode usar esta opção para executar uma tarefa para uma sub-rede específica. Por exemplo, convém instalar um determinado aplicativo em dispositivos de contadores ou verificar dispositivos em uma sub-rede que provavelmente está infectada.

   - **Atribuir tarefa a uma seleção de dispositivo**

     A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar um das opções existentes:

Por exemplo, você pode usar esta opção para executar uma tarefa em dispositivos com uma versão específica do sistema operacional.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada.

5. Na etapa **Escopo da tarefa**, especifique um grupo de administração, dispositivos com endereços específicos ou uma seleção de dispositivos.

   Os ajustes disponíveis dependem da opção selecionada na etapa anterior.

6. Definir os ajustes da tarefa:

   a. No campo **Comando executável**, especifique o comando a ser executado no dispositivo local.

   b. Se necessário, especifique os argumentos da linha de comando no campo **Argumentos da linha de comando (opcionais)**.

   c. Se necessário, especifique o caminho para o arquivo executável no campo **Caminho para a pasta de trabalho (opcional)**.

7. Na etapa **Concluir a criação da tarefa**, clique no botão **Concluir** para criar a tarefa e fechar o assistente.

   Se você ativou a opção **Abrir detalhes da tarefa quando a criação estiver concluída**, a janela de ajustes da tarefa é aberta. Nessa janela, você pode verificar os parâmetros da tarefa, modificá-los ou configurar um agendamento de início de tarefa, se necessário.

8. Clique na nova tarefa.

   A janela de propriedades da tarefa é aberta.

9. Selecione a guia **Agendamento**.

10. Configure o agendamento de tarefas.

> **Nota:** Assegure-se de que o computador esteja ligado para executar a tarefa.

11. Clique em **Salvar**.

12. Para executar a tarefa imediatamente, independentemente do agendamento configurado, faça o seguinte:

    a. Marque a caixa de seleção ao lado da tarefa.

    b. Clique no botão **Executar**.

Consequentemente, o Kaspersky Endpoint Security executa o comando no modo silencioso e inicia o processo. Você pode exibir os resultados da tarefa nas propriedades da tarefa na seção **Resultados da execução**.

Encerrar processo

Você pode encerrar processos remotamente usando a tarefa *Encerrar processo*. Por exemplo, você pode encerrar remotamente um utilitário de teste de velocidade da Internet que foi iniciado usando a tarefa Iniciar processo.

Se você quiser proibir a execução de um arquivo, poderá configurar o componente Prevenção de execução. Você pode proibir a execução de arquivos executáveis, scripts, arquivos no formato do Office.

A tarefa *Encerrar processo* tem as seguintes limitações:

- Você pode configurar a tarefa apenas para EDR Optimum no Web Console.

Para criar uma tarefa Encerrar processo:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** > **Tarefas**.

   A lista de tarefas é aberta.

2. Clique em **Adicionar**.

   O **Assistente para novas tarefas** é iniciado.

3. Definir os ajustes da tarefa:

   a. Na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Mac (12.2.1).

   b. Na lista suspensa **Tipo de tarefa**, selecione **Encerrar processo**.

   c. No campo **Nome da tarefa**, insira uma breve descrição.

   d. Selecione uma das seguintes opções:

   - **Atribuir tarefa a um grupo de administração**

     A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo.

     Por exemplo, você pode querer usar esta opção para executar uma tarefa de enviar uma mensagem aos usuários se a mensagem for específica para dispositivos incluídos em um grupo de administração específico.

     Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas aos ajustes de segurança dos grupos aos quais se aplicam.

   - **Especificar endereços de dispositivo manualmente ou importar endereços de uma lista**

     Você pode especificar nomes NetBIOS, nomes DNS, endereços IP e sub-redes IP de dispositivos aos quais deseja atribuir a tarefa.

     Você pode usar esta opção para executar uma tarefa para uma sub-rede específica. Por exemplo, convém instalar um determinado aplicativo em dispositivos de contadores ou verificar dispositivos em uma sub-rede que provavelmente está infectada.

   - **Atribuir tarefa a uma seleção de dispositivo**

     A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar um das opções existentes:

     Por exemplo, você pode usar esta opção para executar uma tarefa em dispositivos com uma versão específica do sistema operacional.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada.

5. Na etapa **Escopo da tarefa**, especifique um grupo de administração, dispositivos com endereços específicos ou uma seleção de dispositivos.

   Os ajustes disponíveis dependem da opção selecionada na etapa anterior.

6. Nesta etapa do assistente, na lista suspensa **Especifique o arquivo para o qual os processos devem ser encerrados**, selecione uma das opções e preencha os campos necessários. Para especificar o arquivo, você deve inserir o caminho completo para o arquivo ou o hash do arquivo e o caminho.

   Nota: Se você estiver criando esta tarefa para um dispositivo local, poderá especificar o processo por PID.

7. Se você quiser que seja possível aplicar a tarefa a objetos críticos do sistema, marque a caixa de seleção **Aplicar aos objetos críticos do sistema**.

8. Insira as credenciais da conta do usuário cujos direitos você deseja usar para executar a tarefa. Clique em **Avançar**.

   Nota: Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (raiz).

9. Na etapa **Concluir a criação da tarefa**, clique no botão **Concluir** para criar a tarefa e fechar o assistente.

   Se você ativou a opção **Abrir detalhes da tarefa quando a criação estiver concluída**, a janela de ajustes da tarefa é aberta. Nessa janela, você pode verificar os parâmetros da tarefa, modificá-los ou configurar um agendamento de início de tarefa, se necessário.

10. Clique na nova tarefa.

    A janela de propriedades da tarefa é aberta.

11. Selecione a guia **Agendamento**.

12. Configure o agendamento de tarefas.

    Nota: Assegure-se de que o computador esteja ligado para executar a tarefa.

13. Clique em **Salvar**.

14. Para executar a tarefa imediatamente, independentemente do agendamento configurado, faça o seguinte:

    a. Marque a caixa de seleção ao lado da tarefa.

    b. Clique no botão **Executar**.

Como resultado, o Kaspersky Endpoint Security finaliza o processo no computador. Por exemplo, se um aplicativo de *Jogo* estiver em execução e você encerrar o processo de *Jogo*, o aplicativo será fechado sem salvar os dados. Você pode exibir os resultados da tarefa nas propriedades da tarefa na seção **Resultados**.

Prevenção de execução

A prevenção de execução permite gerenciar a execução de arquivos executáveis e scripts, assim como abrir arquivos no formato do Office. Dessa forma, você pode, por exemplo, impedir a execução de aplicativos que considera inseguros. Como resultado, a disseminação da ameaça pode ser interrompida. A prevenção de execução dá suporte a um conjunto de interpretadores de script.

Regra de prevenção de execução

A prevenção de execução gerencia o acesso do usuário a arquivos com regras de prevenção de execução. A regra de prevenção de execução é um conjunto de critérios que o aplicativo leva em consideração ao reagir à execução de um objeto, por exemplo, ao bloquear a execução do objeto. O aplicativo identifica arquivos por seus caminhos ou somas de verificação calculadas usando algoritmos de hash MD5 e SHA256.

Você pode criar regras de Prevenção de execução:

- Nos detalhes do alerta (somente para EDR Optimum).

  Detalhes do alerta é uma ferramenta para exibir a totalidade das informações coletadas sobre uma ameaça detectada. Os detalhes do alerta incluem, por exemplo, o histórico de arquivos que aparecem no computador. Para obter detalhes sobre o gerenciamento de detalhes do alerta, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum.

- Usando uma política de grupo ou ajustes locais do aplicativo. Você deve inserir o caminho do arquivo ou o hash (SHA256 ou MD5), ou ambos, o caminho do arquivo e o hash do arquivo.

Você também pode gerenciar a Prevenção de execução localmente usando a linha de comando.

Nota: É impossível bloquear a inicialização de objetos críticos do sistema (SCO). SCOs são arquivos que o sistema operacional e o aplicativo Kaspersky Endpoint Security for Mac requerem para serem executados.

Modos de regra de prevenção de execução

O componente Prevenção de execução pode funcionar em dois modos:

- **Somente estatísticas**

  Nesse modo, o Kaspersky Endpoint Security publica um evento sobre tentativas de executar objetos executáveis ou documentos abertos que correspondem aos critérios da regra de prevenção no log de eventos do Kaspersky Security Center e no sistema de login unificado, mas não bloqueia a tentativa de executar ou abrir o objeto ou documento. Este modo está marcado por padrão.

- **Ativa**

  Nesse modo, o aplicativo bloqueia a execução de objetos ou a abertura de documentos que atendem aos critérios da regra de prevenção. O aplicativo também publica um evento sobre tentativas de executar objetos ou abrir documentos no log de eventos do Kaspersky Security Center e no sistema de login unificado.

Gerenciar a prevenção de execução

Importante: você pode definir os ajustes do componente somente no Web Console.

Para prevenir a execução:

1. Na janela principal do Web Console, selecione **Dispositivos** > **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Endpoint Security for Mac.

   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Detection and Response** > **Endpoint Detection and Response**.
5. Ative o botão de alternância **Prevenção de Execução**.
6. No bloco **Ação na execução ou abertura de objeto proibido**, selecione o modo de operação do componente:

   - **Bloquear e gravar no relatório**. Nesse modo, o aplicativo bloqueia a execução de objetos ou a abertura de documentos que atendem aos critérios da regra de prevenção. O aplicativo também publica um evento sobre tentativas de executar objetos ou abrir documentos no log de eventos do Kaspersky Security Center e no sistema de login unificado.
   - **Criar log de eventos apenas**. Nesse modo, o Kaspersky Endpoint Security publica um evento sobre tentativas de executar objetos executáveis ou documentos abertos que correspondem aos critérios da regra de prevenção no log de eventos do Kaspersky Security Center e no sistema de login unificado, mas não bloqueia a tentativa de executar ou abrir o objeto ou documento. Este modo está marcado por padrão.
7. Crie uma lista de regras de prevenção de execução:

   a. Clique em **Adicionar**.

   b. Na caixa de diálogo exibida, insira o nome da regra de prevenção de execução (por exemplo, Aplicativo A).

   c. Na lista suspensa **Tipo**, selecione o objeto que deseja bloquear: **Aplicativo**, **Script**, **Documento**.

   Caso selecione um tipo de objeto incorreto, o Kaspersky Endpoint Security não bloqueia o arquivo ou o script.

   d. Para adicionar o arquivo, você deve inserir o hash do arquivo (SHA256 ou MD5), o caminho completo para o arquivo ou o hash e o caminho.

Nota: Se o arquivo estiver localizado em uma unidade de rede, insira o caminho do arquivo da seguinte maneira: /Volumes/shared_folder_name/filename. Caso o caminho do arquivo contenha uma letra de unidade de rede, o Kaspersky Endpoint Security não bloqueia o arquivo ou script.

a. Clique em **OK**.

8. Salve suas alterações.

Consequentemente, o Kaspersky Endpoint Security bloqueia a execução de objetos: execução de arquivos executáveis e scripts, abertura de arquivos em formato office. No entanto, você pode, por exemplo, abrir um arquivo de script em um editor de texto mesmo se a execução do script for impedida. Ao bloquear a execução de um objeto, o Kaspersky Endpoint Security exibe uma notificação padrão se as notificações estiverem ativadas nos ajustes do aplicativo.

Isolamento da rede de computadores

O isolamento da rede de computadores permite isolar automaticamente um computador da rede em resposta à detecção de um indicador de comprometimento (IOC) — este é o modo automático. Você pode ativar o isolamento de rede manualmente enquanto estiver investigando a ameaça detectada — este é o modo manual.

Quando o isolamento de rede está ativado, o aplicativo corta todas as conexões ativas e bloqueia todas as novas conexões de rede TCP/IP no computador, exceto as seguintes conexões:

- Conexões listadas em Exclusões de isolamento de rede.
- Conexões iniciadas pelos serviços do Kaspersky Endpoint Security.
- Conexões iniciadas pelo Agente de Rede do Kaspersky Security Center.

Importante: você pode definir os ajustes do componente somente no Web Console.

Modo de isolamento de rede automático

Você pode configurar o isolamento de rede para ser ativado automaticamente em resposta a uma detecção de IOC. Você pode configurar o modo de isolamento de rede automático com uma política de grupo.

Como configurar o isolamento de rede para ser ativado automaticamente em resposta a uma detecção de IOC

1. Na janela principal do Web Console, selecione **Dispositivos** > **Tarefas**.
2. A lista de tarefas é aberta.
3. Clique na tarefa **Verificação de IOC** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é aberta.

   Se necessário, crie a tarefa de Verificação de IOC.
4. Selecione a guia **Configurações do aplicativo**.

5. No bloco **Ação ao detectar IOC**, selecione a opção **Alertar e adotar ações de resposta após um IOC ser encontrado** e, em seguida, a caixa de seleção **Isolar o computador da rede (8 horas)**.

6. Salve suas alterações.

7. Como resultado, quando um IOC é detectado, o aplicativo isola o computador da rede para impedir que a ameaça se espalhe.

Você pode configurar o isolamento de rede para ser desativado automaticamente após decorrido um tempo especificado. Por padrão, o aplicativo desativa o isolamento de rede após 8 horas desde o momento em que foi ativado. Você também pode desativar o isolamento de rede manualmente (consulte as instruções abaixo). Depois de desativar o isolamento de rede, o computador pode usar a Rede sem restrições.

Como configurar o atraso para desativar o isolamento de rede de um computador no modo automático

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

2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é aberta.

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

4. Vá para **Detection and Response** > **Endpoint Detection and Response**.

5. No bloco **Isolamento de rede**, clique em **Definir os ajustes de desbloqueio do computador**.

6. Na janela exibida, marque a caixa de seleção **Desbloquear automaticamente o computador isolado em** e insira o atraso para desativar automaticamente o isolamento de rede.

7. Salve suas alterações.

Modo de isolamento de rede manual

Você pode ativar e desativar manualmente o isolamento de rede. Você pode configurar o modo de Isolamento de rede manual usando as propriedades do computador no console do Kaspersky Security Center.

Você pode ativar o Isolamento de rede:

- Nos detalhes do alerta (somente para EDR Optimum).

  Detalhes do alerta é uma ferramenta para exibir a totalidade das informações coletadas sobre uma ameaça detectada. Os detalhes do alerta incluem, por exemplo, o histórico de arquivos que aparecem no computador. Para obter detalhes sobre o gerenciamento de detalhes do alerta, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum.

- Usando os ajustes locais do aplicativo.

Como ativar o isolamento de rede de um computador manualmente

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

2. Selecione o computador para o qual você deseja definir os ajustes locais do aplicativo.

   Isso abre as propriedades do computador.

3. Selecione a guia **Aplicativos**.
4. Clique em **Kaspersky Endpoint Security for Mac**.
   Isso abre os ajustes locais do aplicativo.
5. Selecione a guia **Configurações do aplicativo**.
6. Vá para **Detection and Response** > **Endpoint Detection and Response**.
7. No bloco **Isolamento de rede**, clique em **Isolar o computador da rede**.

Você pode configurar o isolamento de rede para ser desativado automaticamente após decorrido um tempo especificado. Por padrão, o aplicativo desativa o isolamento de rede após 8 horas desde o momento em que foi ativado. Depois de desativar o isolamento de rede, o computador pode usar a Rede sem restrições.

Como configurar o atraso para desativar o isolamento de rede de um computador no modo manual

1. Na janela principal do Web Console, selecione **Dispositivos** > **Dispositivos gerenciados**.
2. Selecione o computador para o qual você deseja definir os ajustes locais do aplicativo.
   Isso abre as propriedades do computador.
3. Selecione a guia **Tarefas**.
   Isso exibe a lista de tarefas disponíveis no computador.
4. Selecione a tarefa **Isolamento de rede**.
5. Selecione a guia **Configurações do aplicativo**.
6. Na janela exibida, selecione o atraso para desativar o isolamento de rede.
7. Salve suas alterações.

Como desativar o isolamento de rede de um computador manualmente

1. Na janela principal do Web Console, selecione **Dispositivos** > **Dispositivos gerenciados**.
2. Selecione o computador para o qual você deseja definir os ajustes locais do aplicativo.
3. Isso abre as propriedades do computador.
4. Selecione a guia **Aplicativos**.
5. Clique em Kaspersky Endpoint Security for Mac.
6. Isso abre os ajustes locais do aplicativo.
7. Selecione a guia **Configurações do aplicativo**.
8. Vá para **Detection and Response** > **Endpoint Detection and Response**.
9. No bloco **Isolamento de rede**, clique em **Desbloquear o computador isolado da rede**.

Você também pode desativar o isolamento de rede localmente usando a linha de comando.

Exclusões de isolamento de rede

Você pode configurar exclusões de isolamento de rede. As conexões de rede que correspondem às regras não são bloqueadas no computador quando o isolamento de rede está ativado.

Para configurar as exclusões de isolamento de rede, você pode usar uma lista de perfis de rede padrão. Por padrão, as exclusões incluem perfis de rede que contêm regras que garantem a operação ininterrupta de dispositivos com as funções de servidor DNS/DHCP e cliente DNS/DHCP. Você também pode modificar os ajustes dos perfis de rede padrão ou definir exclusões manualmente (consulte as instruções abaixo).

Importante: as exclusões especificadas nas propriedades da política são aplicadas somente se o isolamento de rede for ativado automaticamente em resposta a uma ameaça detectada. As exclusões especificadas nas propriedades do computador são aplicadas somente se o isolamento de rede estiver ativado manualmente nas propriedades do computador no console do Kaspersky Security Center.

Nota: Uma política ativa não impede a aplicação de exclusões do Isolamento de rede configurado nas propriedades do computador porque esses parâmetros têm cenários de uso diferentes.

Como adicionar uma exclusão de isolamento de rede no modo automático

1. Na janela principal do Web Console, selecione **Dispositivos** > **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Endpoint Security.
3. A janela de propriedades da política é aberta.
4. Selecione a guia **Configurações do aplicativo**.
5. Vá para **Detection and Response** > **Endpoint Detection and Response**.
6. No bloco **Exclusões de isolamento de rede**, clique em **Exclusões**.
7. Na janela seguinte, clique em **Adicionar do perfil** e selecione os perfis de rede padrão para configurar as exclusões.
8. As exclusões de isolamento de rede do perfil são adicionadas à lista de Exclusões de isolamento de rede. Você pode exibir as propriedades das conexões de rede. Se necessário, você pode modificar os ajustes de conexão de rede.
9. Se necessário, adicione uma exclusão de isolamento de rede manualmente. Para fazer isso, na janela com a lista de exclusões, clique em **Adicionar** e edite manualmente os ajustes de conexão de rede.
10. Salve suas alterações.

Como adicionar uma exclusão de isolamento de rede no modo manual

1. Na janela principal do Web Console, selecione **Dispositivos** > **Dispositivos gerenciados**.
2. Selecione o computador para o qual você deseja definir os ajustes locais do aplicativo.
3. Isso abre as propriedades do computador.

4. Selecione a guia **Tarefas**.
5. Isso exibe a lista de tarefas disponíveis no computador.
6. Selecione a tarefa **Isolamento de rede**.
7. Selecione a guia **Configurações do aplicativo**.
8. Na janela exibida, clique em **Exclusões**.
9. Na janela seguinte, clique em **Adicionar do perfil** e selecione os perfis de rede padrão para configurar as exclusões.
10. As exclusões de isolamento de rede do perfil são adicionadas à lista de Exclusões de isolamento de rede. Você pode exibir as propriedades das conexões de rede. Se necessário, você pode modificar os ajustes de conexão de rede.
11. Se necessário, adicione uma exclusão de isolamento de rede manualmente. Para fazer isso, na janela com a lista de exclusões, clique em **Adicionar** e edite manualmente os ajustes de conexão de rede.
12. Salve suas alterações.

Você também pode exibir a lista de Exclusão de isolamento de rede localmente usando a linha de comando. Nesse caso, o computador deve ser isolado.

Cloud Sandbox

Cloud Sandbox é uma tecnologia que permite detectar ameaças avançadas em um computador. O Kaspersky Endpoint Security encaminha automaticamente arquivos detectados para a Cloud Sandbox analisar. O Cloud Sandbox executa esses arquivos em um ambiente isolado para identificar atividades maliciosas e avaliar a sua reputação. Os dados nesses arquivos são então enviados para a Kaspersky Security Network. Portanto, caso o Cloud Sandbox detecte um arquivo malicioso, o Kaspersky Endpoint Security executará a ação pertinente para eliminar essa ameaça em todos os computadores onde esse arquivo for detectado.

Importante: para que o Cloud Sandbox funcione, você deve ativar o uso do Kaspersky Security Network.

Nota: se você estiver usando o Kaspersky Private Security Network, a tecnologia Cloud Sandbox não estará disponível.

Para ativar o Cloud Sandbox:

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para a seção **Configuração de agentes integrados → Endpoint Detection and Response**.
5. Selecione a guia **Cloud Sandbox**.

6. Ative o botão de alternância do **Cloud Sandbox**.

7. Salve suas alterações.

Sempre que houver uma ameaça, o Kaspersky Endpoint Security ativa o contador de ameaças detectadas usando o Cloud Sandbox na janela principal do aplicativo na seção **Detecção de ameaças**. O Kaspersky Endpoint Security também indicará a tecnologia de detecção de ameaças Cloud Sandbox no Relatório sobre ameaças no console do Kaspersky Security Center.

Criptografia de disco FileVault

O Kaspersky Endpoint Security permite que a criptografia do FileVault seja gerenciada remotamente. A criptografia impede que usuários não autorizados acessem dados confidenciais armazenados no disco de inicialização do computador do usuário.

Quando um administrador inicia a criptografia do FileVault em um computador a partir do Kaspersky Security Center, o Kaspersky Endpoint Security solicita que um usuário de tal computador insira suas credenciais. A criptografia do disco será iniciada somente após o usuário fornecer as credenciais, o computador ser reiniciado e 30 minutos se passarem desde que os ajustes de política foram recebidos no computador. O intervalo mínimo entre solicitações de credenciais também é de 30 minutos.

Para impedir que o usuário descriptografe o disco de inicialização do Mac quando a criptografia do FileVault estiver ativada, um administrador precisa usar o JAMF para implementar um perfil MDM que proíbe a descriptografia do disco. Para descriptografar o disco de inicialização de um Mac com um perfil MDM que proíbe a descriptografia do disco, o administrador precisa primeiro remover o perfil.

Nota: se o gerenciamento de criptografia do FileVault não estiver ativado no Kaspersky Security Center, os usuários com direitos de administrador poderão criptografar e descriptografar os discos de inicialização do Mac no Ajuste do Sistema. Para obter mais informações sobre o FileVault, consulte a documentação da Apple.

Se o computador tiver várias contas, a criptografia do FileVault torna o disco inacessível a todos os usuários, exceto ao usuário que inseriu as próprias credenciais.

Permitir que outros usuários desbloqueiem o disco

1. Escolha o **menu Apple** > **Ajuste do Sistema** > **Privacidade e Segurança**.

2. Clique em **FileVault**.

   A janela **FileVault** é aberta.

3. Clique em **Habilitar usuários**.

4. Na janela exibida, selecione um usuário para autorizar o desbloqueio do computador.

5. Insira a senha da conta de computador do usuário e clique em **OK**.

6. Clique em **Continuar**.

O usuário pode acessar o disco criptografado.

Nota: são necessários direitos de administrador para permitir que outros usuários desbloqueiem o disco.

Se um administrador gerenciar o Kaspersky Endpoint Security por meio do Kaspersky Security Center Administration Console, Web Console ou Cloud Console, e um usuário desse computador esquecer ou perder as suas credenciais e não puder acessar um disco criptografado, o administrador poderá obter uma chave de recuperação.

Como obter uma chave de recuperação usando o Console de Administração do Kaspersky Security Center

Como obter uma chave de recuperação usando o Kaspersky Security Center Web Console e o Cloud Console

Proteção por senha

O Kaspersky Endpoint Security permite limitar ações indesejadas nos dispositivos dos usuários definindo uma senha de administrador.

Se a Proteção por senha estiver ativada, o Kaspersky Endpoint Security exigirá uma senha ao tentar executar qualquer uma das seguintes ações:

- Configurar os ajustes do aplicativo
- Sair do aplicativo
- Remover a chave de licença
- Remover o aplicativo

  > **Nota:** A proteção por senha restringe a remoção do Kaspersky Endpoint Security somente quando executada por meio do desinstalador.

- Restaurar arquivos em quarentena do Backup
- Visualizar relatórios.

Desativar a Proteção por senha não desativa os ajustes da política. Se a edição de um ajuste for proibida na política, ela não poderá ser editada mesmo se a Proteção por senha estiver desativada.

Ative a Proteção por senha usando o Console de Administração

1. Inicie o Console de Administração.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Na área de trabalho, selecione a guia **Políticas**.
5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
6. Na janela **Propriedades**, selecione **Configurações adicionais > Interação do usuário**.
7. Na seção **Proteção por senha**, marque a caixa de seleção **Ativar a proteção por senha**.

8. Na janela exibida, **Configurações de proteção por senha**, defina os seguintes ajustes:

    - Insira a senha no campo **Senha** e repita a senha uma segunda vez no campo **Confirmar senha**.
    - Na seção **Exigir senha para**, marque as caixas de seleção necessárias para proteger as ações correspondentes no dispositivo do usuário.

9. Clique em **OK** para salvar suas alterações.
10. Siga um destes procedimentos para aplicar as alterações à política:

    - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da política>** após salvar as alterações.
    - Clique em **OK** para fechar a janela **Propriedades: <Nome da política>** após salvar as alterações.

Edite os ajustes de Proteção por senha usando o Console de Administração

1. Inicie o Console de Administração.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Na área de trabalho, selecione a guia **Políticas**.
5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
6. Na janela **Propriedades**, selecione **Configurações adicionais > Interação do usuário**.
7. Na seção **Proteção por senha**, clique no botão **Configurações**.
8. Na janela **Configurações de proteção por senha** exibida, edite as configurações que deseja alterar.
9. Clique em **OK** para salvar suas alterações.

Ativar a Proteção por senha usando o Web Console

1. Na janela principal do Web Console, selecione **Dispositivos** > **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Endpoint Security for Mac.
3. A janela de propriedades da política é aberta.
4. Selecione a guia **Configurações do aplicativo**.
5. Selecione **Ajustes adicionais** > **Interação do usuário**.
6. Ative o botão de alternância **Proteção por senha**.
7. Na janela exibida, **Ajustes de proteção por senha**, defina os seguintes ajustes:

    - Insira a senha no campo **Senha** e repita a senha uma segunda vez no campo **Confirmar senha**. Por padrão, os caracteres da senha ficam ocultos por motivo de segurança. Para exibir a senha, clique em **Exibir**.
    - Na seção **Requer senha para**, marque as caixas de seleção necessárias para proteger as ações correspondentes no dispositivo do usuário.

8. Clique em **OK** para fechar a caixa de diálogo **Ajustes de proteção por senha**.
9. Clique em **OK** para fechar a seção **Interação do usuário**.
10. Clique em **Salvar** para salvar as alterações na política.

Editar Proteção por senha usando o Web Console

1. Na janela principal do Web Console, selecione **Dispositivos** > **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Endpoint Security for Mac.
3. A janela de propriedades da política é aberta.
4. Selecione a guia **Configurações do aplicativo**.
5. Selecione **Ajustes adicionais** > **Interação do usuário**.
6. Na seção **Proteção por senha**, clique no botão **Configurações**.
7. Na caixa de diálogo **Ajustes de proteção por senha** exibida, edite as configurações que deseja alterar.
8. Clique em **OK** para fechar a caixa de diálogo **Ajustes de proteção por senha**.
9. Clique em **OK** para fechar a seção **Interação do usuário**.
10. Clique em **Salvar** para salvar as alterações na política.

Ative a Proteção por senha usando o aplicativo Kaspersky Endpoint Security

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.
   É aberta a janela de ajustes do aplicativo.
2. Na guia **Interface**, na seção **Proteção por senha**, marque a caixa de seleção **Ativar a proteção por senha**.
3. Na janela exibida, defina os seguintes ajustes:
   - Insira a senha no campo **Senha** e repita a senha uma segunda vez no campo **Confirmar senha**.
   - Na seção **Exigir senha para**, marque as caixas de seleção necessárias para proteger as ações correspondentes no dispositivo do usuário.
4. Clique em **OK**.

> **Nota:** Se você selecionar **Alterar ajustes do aplicativo** como uma ação protegida por senha, será necessário inserir a senha duas vezes para alterar as configurações de Proteção por senha.

Editar Proteção por senha usando o aplicativo Kaspersky Endpoint Security

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.
   É aberta a janela de ajustes do aplicativo.
2. Na guia **Interface**, na seção **Proteção por senha**, clique em **Ajustes**.

3. Na janela exibida, edite os ajustes que deseja alterar.

4. Clique em **OK**.

Prevenção de Exploits

O componente de Prevenção de Exploits detecta o código do programa que aproveita as vulnerabilidades no computador para explorar privilégios de administrador ou executar atividades maliciosas. Por exemplo, os exploits podem utilizar um ataque de estouro de buffer. Para isso, o exploit envia uma grande quantidade de dados para um aplicativo vulnerável. Ao processar esses dados, o aplicativo vulnerável executa um código malicioso. Como resultado desse ataque, o exploit pode iniciar uma instalação não autorizada de malware. Quando há uma tentativa de executar um arquivo executável de um aplicativo vulnerável que não foi realizada pelo usuário, o Kaspersky Endpoint Security bloqueia a execução do arquivo ou notifica o usuário.

Por padrão, a Prevenção de Exploits está ativada. Caso necessário, é possível desativar a Prevenção de Exploits.

Ativar/desativar a Prevenção de Exploits pelo Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.

2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é aberta.

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

4. Vá para a seção **Proteção Contra Ameaças ao Host → Análise de comportamento → Prevenção de Exploits**.

5. Ative ou desative o componente usando botão de alternância **Prevenção de Exploits**.

6. Caso a Prevenção de Exploits esteja ativada, selecione uma das seguintes ações a ser executada quando a atividade de exploits for detectada:

   - **Bloquear**

     Se esse item for selecionado ao detectar uma exploit, o Kaspersky Endpoint Security bloqueará as operações dessa exploit e registrará as informações sobre ela.

   - **Informar**

     Caso este item seja selecionado, quando o Kaspersky Endpoint Security detectar um exploit, ele registrará uma entrada contendo as informações sobre o exploit e adicionará essas informações na lista de ameaças ativas.

7. Salve suas alterações.

Ativar/desativar a Prevenção de Exploits pelo Console de Administração

1. Inicie o Console de Administração.

2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.

3. Na árvore do console, clique em **Dispositivos gerenciados**.

4. Na área de trabalho, selecione a guia **Políticas**.
5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
6. Na janela **Propriedades**, selecione **Proteção Avançada Contra Ameaças** > **Prevenção de Exploits**.
7. Marque ou desmarque a caixa **Ativar a Prevenção contra Exploração**.
8. Se necessário, na seção **Ao detectar exploit**, selecione a ação a ser executada quando o Kaspersky Endpoint Security detectar um exploit.
9. Clique em **OK** para salvar suas alterações.
10. Siga um destes procedimentos para aplicar as alterações à política:
    - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da política>** após salvar as alterações.
    - Clique em **OK** para fechar a janela **Propriedades: <Nome da política>** após salvar as alterações.

Ative/desative a Prevenção de Exploits pelo aplicativo Kaspersky Endpoint Security

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.
2. Na guia **Avançado**, na seção Prevenção de Exploits, marque ou desmarque a caixa **Ativar a Prevenção contra Exploração**.
3. Caso a caixa de seleção **Ativar Detecção de Comportamento** estiver marcada, selecione uma das seguintes ações a ser executada quando a atividade de malware for detectada:
    - **Bloquear automaticamente as atividades perigosas de malware**

      Se esse item for selecionado ao detectar uma exploit, o Kaspersky Endpoint Security bloqueará as operações dessa exploit e registrará as informações sobre ela.
    - **Informar**

      Caso este item seja selecionado, quando o Kaspersky Endpoint Security detectar um exploit, ele registrará uma entrada contendo as informações sobre o exploit e adicionará essas informações na lista de ameaças ativas.

Exibir o relatório da Prevenção de Exploits

1. Na barra de menus, selecione **Proteção** > **Relatórios**.

   Será exibida a janela **Relatórios**.
2. Abra a guia **Prevenção de Exploits**.

Mecanismo de Remediação

O Mecanismo de Remediação permite que o Kaspersky Endpoint Security desfaça ações executadas por Malwares no sistema operacional.

Ao reverter a atividade de Malware no sistema operacional, o Kaspersky Endpoint Security processa os seguintes tipos da atividade de Malware:

- **Atividade de arquivos**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Exclui arquivos executáveis que foram criados por malware (em todas as mídias, exceto unidades de rede).
  - Exclui arquivos executáveis que foram criados por programas infiltrados por malware.
  - Restaura arquivos que foram modificados ou excluídos por malware.

- **Atividade do sistema**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Encerra os processos que foram iniciados por malware.
  - Encerra os processos nos quais um aplicativo malicioso foi injetado.
  - Não retoma processos que foram interrompidos por malware.

- **Atividade de rede**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Bloqueia a atividade de rede do malware.

Uma reversão de ações de malware pode ser iniciada pelo componente Proteção Contra Ameaças ao Arquivo ou Detecção de Comportamento, ou durante uma verificação de malware.

A reversão de operações de malware afeta um conjunto de dados estritamente definido. A reversão não tem efeitos adversos no sistema operacional ou na integridade dos dados do computador.

Ativar/desativar o Mecanismo de Remediação no Console de Administração

1. Inicie o Console de Administração.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Na área de trabalho, selecione a guia **Políticas**.
5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
6. Na janela **Propriedades**, selecione **Proteção Avançada Contra Ameaças** > **Mecanismo de Remediação**.
7. Marque ou desmarque a caixa de seleção **Ativar o Mecanismo de Remediação**.
8. Clique em **OK** para salvar suas alterações.

9. Siga um destes procedimentos para aplicar as alterações à política:

   - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da política>** após salvar as alterações.
   - Clique em **OK** para fechar a janela **Propriedades: <Nome da política>** após salvar as alterações.

Ativar/desativar o Mecanismo de Remediação no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para a seção **Proteção Contra Ameaças ao Host → Análise de comportamento → Mecanismo de Remediação**.
5. Ative ou desative o componente usando o botão de alternância **Mecanismo de Remediação**.
6. Salve suas alterações.

Ativar/desativar o Mecanismo de Remediação na interface do aplicativo

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.
2. Na guia **Avançado**, na seção **Mecanismo de Remediação**, marque ou desmarque a caixa de seleção **Ativar o Mecanismo de Remediação**.

Como resultado, se o Mecanismo de Remediação estiver ativado, o Kaspersky Endpoint Security reverterá as ações executadas por aplicativos maliciosos no sistema operacional.

Controle da Web

O Controle da Web gerencia o acesso dos usuários aos recursos da Web. Isso ajuda a reduzir o tráfego e o uso inadequado do tempo de trabalho. Quando um usuário tenta abrir um site restrito pelo Controle da Web, o Kaspersky Endpoint Security bloqueará o acesso ou exibirá um aviso.

Você pode bloquear o acesso a sites específicos ou categorias selecionadas de sites.

Nota: o aplicativo Kaspersky Endpoint Security só pode bloquear o acesso a sites que usam HTTPS para conexões. O Kaspersky Endpoint Security verifica as conexões criptografadas (HTTPS) somente se a caixa de seleção **Verificar conexões seguras (HTTPS)** na seção **Essencial** na guia **Geral** estiver marcada.

Adicionar uma nova regra no Console de Administração

1. Inicie o Console de Administração.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.

4. Na área de trabalho, selecione a guia **Políticas**.
5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
6. Na janela **Propriedades**, selecione **Controles de Segurança** > **Controle da Web**.
7. Marque a caixa de seleção **Ativar Controle da Web**.
8. Clique em **Adicionar**.
9. Na janela exibida, insira um nome de regra.
10. Se você quiser que a regra esteja ativa, marque a caixa de seleção **Regra ativa**.
11. Siga um destes procedimentos:
    - Se você quiser que a regra se aplique a endereços da Web específicos, selecione a opção **Endereços da Web ou um grupo de endereços da Web por máscara**.
    - Se você quiser que a regra seja aplicada a categorias de sites específicas, selecione a opção **Categorias de site**.
12. Clique em **Especificar**.
13. Na janela exibida, especifique o escopo da regra.
14. Siga um destes procedimentos:
    - Se você quiser que o Kaspersky Endpoint Security bloqueie o acesso, selecione a opção **Bloquear**.
    - Se você quiser que o Kaspersky Endpoint Security permita o acesso, selecione a opção **Permitir**.
    - Se você quiser que o Kaspersky Endpoint Security exiba um aviso, selecione a opção **Exibir aviso**.
15. Clique em **OK** para salvar suas alterações.
16. Siga um destes procedimentos para aplicar as alterações à política:
    - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da política>** após salvar as alterações.
    - Clique em **OK** para fechar a janela **Propriedades: <Nome da política>** após salvar as alterações.

Adicionar uma nova regra no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controles de Segurança → Controle da Web**.
5. Ative o botão de alternância do **Controle da Web**.

6. Clique em **Adicionar**.
7. Na janela exibida, insira um nome de regra.
8. Siga um destes procedimentos:
   - Se você quiser que a regra esteja ativa, selecione a opção **Ativo**.
   - Se você quiser que a regra fique inativa, selecione a opção **Inativo**.
9. Siga um destes procedimentos:
   - Se você quiser que o Kaspersky Endpoint Security permita o acesso, selecione a opção **Permitir**.
   - Se você quiser que o Kaspersky Endpoint Security bloqueie o acesso, selecione a opção **Bloquear**.
   - Se você quiser que o Kaspersky Endpoint Security exiba um aviso, selecione a opção **Exibir aviso**.
10. Siga um destes procedimentos:
    - Se você quiser que a regra seja aplicada a categorias de sites específicas, selecione a opção **Categorias** e clique em **Selecionar categorias** para selecionar as categorias.
    - Se você quiser que a regra se aplique a endereços da Web específicos, selecione a opção **Endereços individuais** e adicione-os à tabela abaixo.
11. Salve suas alterações.

Nota: as configurações do Controle da Web não podem ser gerenciadas no aplicativo Kaspersky Endpoint Security.

Controle de Dispositivos

O Controle de Dispositivos gerencia o acesso dos usuários aos dispositivos instalados ou conectados ao computador. Isso permite proteger o computador contra infecções quando esses dispositivos estão conectados e evitar a perda ou vazamento de dados.

Níveis de acesso ao dispositivo

O Controle de Dispositivos controla o acesso nos seguintes níveis:

- **Tipo de dispositivo**. Você pode controlar o acesso a discos rígidos, discos removíveis, disquetes, unidades de CD/DVD e acesso a redes Wi-Fi.

Você pode configurar o acesso ao dispositivo da seguinte forma:

- Permitir.
- Bloquear.
- Bloquear com exceções (somente Wi-Fi).

- **Dispositivos confiáveis.** Dispositivos confiáveis são dispositivos aos quais os usuários especificados nas configurações de dispositivo confiável têm acesso total permanentemente.

  Você pode adicionar dispositivos confiáveis com base nos seguintes dados:

  - **Dispositivos por ID**. Cada dispositivo tem um ID exclusivo (ID do hardware ou HWID). Você pode exibir o ID nas propriedades do dispositivo usando as ferramentas do sistema operacional. Exemplo de um ID de dispositivo: SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000. Adicionar dispositivos por ID é conveniente se você quiser adicionar vários dispositivos específicos.
  - **Dispositivos por modelo**. Cada dispositivo tem um ID do fornecedor (VID) e um ID do produto (PID). Você pode exibir os IDs nas propriedades do dispositivo usando as ferramentas do sistema operacional. Modelo para inserir o VID e PID: VID_1234&PID_5678. Adicionar dispositivos por modelo é conveniente se você usar dispositivos de um determinado modelo em sua organização. Dessa forma, você pode adicionar todos os dispositivos deste modelo.
  - **Dispositivos por máscara de ID**. Se você estiver usando vários dispositivos com IDs semelhantes, poderá adicionar dispositivos à lista confiável usando máscaras. O caractere `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o caractere `?` ao inserir uma máscara. Por exemplo, `WDC_C*`.
  - **Dispositivos por máscara de modelo**. Se você estiver usando vários dispositivos com VIDs ou PIDs semelhantes (por exemplo, dispositivos do mesmo fabricante), poderá adicionar dispositivos à lista confiável usando máscaras. O caractere `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o caractere `?` ao inserir uma máscara. Por exemplo, `VID_05AC&PID_*`.

Gerenciar o componente Controle de Dispositivos no Console de Administração

1. Inicie o Console de Administração.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Na área de trabalho, selecione a guia **Políticas**.
5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
6. Na janela **Propriedades**, selecione **Controles de Segurança** > **Controle de dispositivos**.
7. Marque a caixa de seleção **Ativar Controle de Dispositivos**.
8. Na guia **Tipos de dispositivos**, configure as regras de acesso para tipos de dispositivos e redes Wi-Fi.
9. Na guia **Dispositivos confiáveis**, configure as regras de acesso para dispositivos individuais ou grupos de dispositivos.
10. Clique em **OK** para salvar suas alterações.

11. Siga um destes procedimentos para aplicar as alterações à política:

    - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da política>** após salvar as alterações.
    - Clique em **OK** para fechar a janela **Propriedades: <Nome da política>** após salvar as alterações.

Gerenciar o componente Controle de Dispositivos no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controles de Segurança** > **Controle de Dispositivos**.
5. Ative o botão de alternância **Controle de Dispositivos**.
6. Na seção **Configurações do Controle de dispositivos**, configure regras de acesso para dispositivos, tipos de dispositivos e redes Wi-Fi.
7. Salve suas alterações.

Nota: as configurações do Controle de Dispositivos não podem ser gerenciadas no aplicativo Kaspersky Endpoint Security.

Como resultado, se o Controle de Dispositivos estiver ativado, o aplicativo retransmitirá as informações sobre os dispositivos conectados ao Kaspersky Security Center. Você pode visualizar a lista de dispositivos conectados no Kaspersky Security Center em **Avançado** → **Repositórios** → **pasta Hardware**.

Visualizar o relatório do Controle de Dispositivos

1. Na barra de menus, selecione **Proteção** > **Relatórios**.

   Será exibida a janela **Relatórios**.
2. Abra a guia **Controle de dispositivos**.

Participar na Kaspersky Security Network

Quando você participa da Kaspersky Security Network, as estatísticas do aplicativo Kaspersky Endpoint Security são enviadas automaticamente para a Kaspersky para aprimorar a proteção do seu Mac.

Nota: a Kaspersky não recebe, processa ou armazena nenhum dado pessoal sem o seu consentimento explícito.

A participação no Kaspersky Security Network é voluntária. A decisão de participar ou não é tomada quando você instala o aplicativo. De qualquer forma, você pode mudar sua decisão posteriormente, a qualquer momento.

Ativar o Kaspersky Security Network

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Avançado**, na seção **KSN**, clique em **Mostrar a Declaração da KSN** para exibir a Declaração da Kaspersky Security Network.

3. Se desejar que o Kaspersky Endpoint Security use informações sobre a reputação de arquivos, os recursos da Web, os aplicativos recebidos da Kaspersky Security Network, e aceitar todos os termos da Declaração, marque a caixa de seleção **Participar da Kaspersky Security Network**.

4. Na janela exibida, clique em **Confirmar**.

   As caixas de seleção **Participar da Kaspersky Security Network** e **Ativar modo KSN estendido** serão selecionadas.

Nota: por padrão, o Kaspersky Endpoint Security usa o modo KSN estendido. O *Modo Estendido da KSN* é um modo no qual o Kaspersky Endpoint Security envia dados adicionais ao Kaspersky. Se você não quiser fornecer esses dados ao Kaspersky, desmarque a caixa de seleção **Ativar modo KSN estendido**.

Dados fornecidos à Kaspersky ao usar a Kaspersky Security Network

Se a caixa de seleção **Participar da Kaspersky Security Network** estiver marcada e a caixa de seleção **Ativar modo KSN estendido** estiver desmarcada, o Kaspersky Endpoint Security fornece à Kaspersky os seguintes dados:

- Informações sobre a licença usada: o tipo e o período de validade da licença, número de dias até a expiração da licença, identificador do parceiro de quem a licença foi adquirida, identificador do Centro de Ativação Regional, soma de verificação do código de ativação, hash do corpo do tíquete calculado usando o algoritmo SHA1, data e hora da criação do tíquete de licença, identificador de informações da licença, identificador do tíquete de licença, identificador da sequência do tíquete de licença, identificador exclusivo do computador do usuário, data a partir da qual o tíquete de licença começa a valer, data de expiração da validade do tíquete de licença, estado atual do tíquete de licença, versão do cabeçalho do tíquete, versão da licença, identificador do certificado de assinatura do cabeçalho do tíquete, soma de verificação do arquivo de chave, número de série do assinante do cabeçalho do tíquete, token de autenticação.

- Versão completa do software instalado;
  tipo do Software instalado;

ID de atualização do Software; ID do serviço de reputação; ID do tipo de protocolo; ID de um centro de ativação regional; versão da lista de decisões revogadas do serviço de Software; ID do registro acionado nos bancos de dados de antivírus do Software; carimbo de data e hora do registro acionado nos bancos de dados de antivírus do Software; tipo do registro acionado nos bancos de dados de antivírus do Software; ID exclusiva da instância da instalação do aplicativo no computador; data de ativação da licença; data de expiração da licença; identificador da licença; status da licença usada pelo Software; tipo de soma de verificação do objeto que está sendo processado; nome do malware detectado ou do software legítimo que pode ser usado para causar danos ao dispositivo ou aos dados do usuário; soma de verificação do objeto que está sendo processado; soma de verificação do código de ativação do Software; versão completa do Software; ID exclusivo do dispositivo; ID do Software; soma de verificação do arquivo da chave do Software; ID do modelo de informações usado para fornecer a licença do Software; identificador do certificado usado para assinar o cabeçalho do tíquete de licença do Software; data e hora de criação do tíquete de licença do Software; a soma de verificação do tíquete de licença do Software; a versão do tíquete de licença do Software; a versão do código de ativação do Software; formato dos dados na solicitação para a infraestrutura do Titular dos Direitos; ID do tíquete de licença atual; o ID de componente do Software; o resultado da ação do Software; código de erro; endereço acessado do serviço Web (URL, IP); número da porta; endereço web da origem da solicitação de serviço da web (referenciador); chave pública do certificado; impressão digital do certificado digital do objeto verificado e algoritmo de hash.

Se as caixas de seleção **Participar da Kaspersky Security Network** e **Ativar modo KSN estendido** estiverem selecionadas, o Kaspersky Endpoint Security fornecerá ao Kaspersky os seguintes dados:

- Informações sobre a versão do sistema operacional (SO) e os service packs instalados no computador, a versão e as somas de verificação (MD5, SHA2-256, SHA1) do arquivo de kernel do SO, parâmetros do modo de execução do SO; versão do SO, número da compilação do SO, número da atualização do SO, edição do SO, informações estendidas sobre a edição do SO; versão do Service Pack do SO; data e hora da inicialização do SO; tempo de atraso do processamento do evento sobre a ação do SO no subsistema de análise comportamental; número de eventos da ação atrasada do SO do tipo atual; tempo de atraso de processamento do evento sobre a ação do SO no subsistema de defesa proativo; número de eventos processadas de ação do SO; número de eventos da ação processada síncrona do SO; atraso total de todos os eventos da ação do SO do tipo atual; tempo de atraso de processamento do evento sobre a ação do SO no subsistema de armazenamento de eventos persistentes; atraso total de todos os eventos da ação do SO; número de eventos da ação em espera síncrona do SO; data e hora do evento recebido de uma ação no SO.

- Informações sobre a última reinicialização do SO com falha: número de reinicializações com falha.

- Informações sobre o aplicativo instalado do Titular dos direitos e o status da proteção antivírus: ID de instalação do Software (PCID); Versão do registro do banco de dados do software; identificados exclusivo da instância da instalação do aplicativo no computador, tipo do aplicativo, ID do tipo do aplicativo, a versão completa do aplicativo instalado, a versão do identificador das configurações do aplicativo, o identificador do tipo de computador, o identificador exclusivo do computador em que o aplicativo está instalado, o identificador exclusivo do Usuário nos serviços do Titular de Direitos, idioma local e estado da operação, versão dos componentes do Software instalado e seus estados de operação, versão do protocolo usado para conectar com os serviços do Titular de Direitos; versão completa do software instalado; tipo do Software instalado; ID de atualização do Software; ID do serviço de reputação; ID do tipo de protocolo; ID de um centro de ativação regional; versão da lista de decisões revogadas do serviço de Software; ID do registro acionado nos bancos de dados de antivírus do Software; carimbo de data e hora do registro acionado nos bancos de dados de antivírus do Software; tipo do registro acionado nos bancos de dados de antivírus do Software; ID exclusiva da instância da instalação do aplicativo no computador; data de ativação da licença; data de expiração da licença; identificador da licença; status da licença usada pelo Software; tipo de soma de verificação do objeto que está sendo processado; nome do malware detectado ou do software legítimo que pode ser usado para causar danos ao dispositivo ou aos dados do usuário; soma de verificação do objeto que está sendo processado; soma de verificação do código de ativação do Software; versão completa do Software; ID do Software; soma de verificação do arquivo da chave do Software; ID do modelo de informações usado para fornecer a licença do Software; identificador do certificado usado para assinar o cabeçalho do tíquete de licença do Software; data e hora de criação do tíquete de licença do Software; a soma de verificação do tíquete de licença do Software; a versão do tíquete de licença do Software; a versão do código de ativação do Software; formato dos dados na solicitação para a infraestrutura do Titular dos Direitos; ID do tíquete de licença atual; o ID de componente do Software; o resultado da ação do Software; código de erro; endereço acessado do serviço Web (URL, IP); número da porta; endereço web da origem da solicitação de serviço da web (referenciador); número de ciclos atualização-aplicação para bases de dados antivírus; data e hora em que as bases de dados de antivírus foram atualizadas e aplicadas pela última vez; data e hora do lançamento nos bancos de dados do Software; versão do componente do Software; ID de atualização do Software; tipo do Software instalado; data e hora da inicialização do Inspetor do Sistema; data e hora da instalação do Software; probabilidade de enviar estatísticas pelo Inspetor do Sistema; código do evento que demorou mais tempo do que o tempo padrão a processar pelo Inspetor do Sistema; tempo de processamento da base de dados do evento que demorou mais tempo do que o tempo padrão a processar pelo Inspetor do Sistema; tempo máximo permitido para processamento de um evento pelo Inspetor do Sistema; tempo de processamento do evento que levou mais tempo do que o padrão para ser processado pelo Inspetor do Sistema; número total de eventos que demoraram mais tempo do que o tempo padrão para processar pelo Inspetor do Sistema.

- Informações sobre todos os objetos e operações processados: Veredito do software sobre o objeto sendo processado; código do diretório; tamanho do objeto que está sendo processado; soma de verificação (SHA256) do objeto que está sendo processado; número do software detectado no contexto do Inspetor do Sistema; data e hora da detecção do software pelo Inspetor do Sistema; detectar características; ID do registro acionado nos bancos de dados de antivírus do Software; motivo da detecção do software pelo Inspetor do Sistema; soma de verificação (MD5) do objeto que está sendo processado; resultado da verificação de integridade do módulo; nome do objeto que está sendo processado; tipo do registro acionado nos bancos de dados de antivírus do Software; caminho para o objeto que está sendo processado; o nome do objeto verificado; a data e hora da verificação; os endereços URL e de referência dos quais foi baixado; o tamanho dos arquivos verificados e os caminhos para eles; o sinal de arquivo; a data e hora da criação do arquivo; o nome, tamanho e somas de verificação (MD5, SHA2-256) do compactador (se o arquivo foi empacotado); a entropia do arquivo; o tipo de arquivo; o código do tipo de arquivo; o sinal, ID e formato do arquivo executável; a soma de verificação do objeto (MD5, SHA2-256); o tipo e o valor da soma de verificação suplementar do objeto; dados sobre a assinatura digital do objeto (certificado): dados sobre o editor do certificado, número de inicializações do objeto desde a última entrega de estatísticas, ID da tarefa de verificação do aplicativo, meio de recebimento de informações sobre a reputação do objeto, valor do filtro alvo, parâmetros técnicos das tecnologias de detecção aplicáveis; caminho para o objeto que está sendo processado; código do diretório.

- Para arquivos executáveis: a entropia das seções do arquivo, indicador de verificação de reputação ou indicador de assinatura de arquivo, nome, tipo, tipo de ID, soma de verificação (MD5) e o tamanho do aplicativo que foi carregado pelo objeto que está sendo validado, o caminho do aplicativo e os caminhos do modelo, um atributo indicando presença na lista de Autorun, data de entrada, lista de atributos, nome do compactador, informações sobre a assinatura digital do aplicativo: o certificado do editor, o nome do arquivo carregado no formato MIME, a data e hora de compilação do arquivo.

- Informações sobre aplicativos iniciados e os seus módulos: somas de verificação (MD5, SHA2-256) de arquivos em execução, tamanho, atributos, data de criação, nome do compactador (se o arquivo foi compactado), nomes de arquivos, informações sobre processos em execução no sistema (ID do processo (PID)), nome do processo, informações sobre a conta a partir da qual o processo foi iniciado, o aplicativo e o comando que iniciaram o processo, o caminho completo para os arquivos do processo e a linha de comando inicial, uma descrição do aplicativo ao qual o processo pertence (o nome do aplicativo e as informações sobre o editor, além dos certificados digitais usados e as informações necessárias para verificar a autenticidade ou as informações sobre a ausência de assinatura digital de um arquivo), e informações sobre os módulos carregados nos processos: seus nomes, tamanhos, tipos, datas de criação, atributos, somas de verificação (MD5, SHA2-256, SHA1), os caminhos para eles, informações do cabeçalho do arquivo PE, nomes dos compactadores (se o arquivo foi compactado), informações sobre a disponibilidade e validade dessas estatísticas, identificador do modo para gerar as estatísticas que estão sendo enviadas.

- Se forem detectadas ameaças ou vulnerabilidades, além das informações sobre o objeto detectado, são fornecidas informações sobre o identificador, a versão e o tipo do registro no banco de dados de antivírus, o nome da ameaça com base na classificação da Kaspersky, a data e hora da última atualização do banco de dados de antivírus, o nome do arquivo executável, a soma de verificação (MD5) do arquivo do aplicativo que solicitou o URL no qual a ameaça foi detectada, o endereço IP (IPv4 ou IPv6) da ameaça detectada, o identificador de vulnerabilidade e seu nível de ameaça, o URL e o referenciador da página da Web em que a vulnerabilidade foi detectada.

- Se um objeto potencialmente malicioso for detectado, são fornecidas informações sobre os dados na memória dos processos.

- Informações sobre ataque de rede: endereço IP do computador atacante e número da porta no computador do usuário visado pelo ataque de rede, ID do protocolo de ataque, nome e tipo de ataque.

- Informações sobre conexões de rede: versão e somas de verificação (MD5, SHA2-256, SHA1) do arquivo a partir do qual foi iniciado o processo que abriu a porta, caminho para o arquivo do processo e a respectiva assinatura digital, endereços IP local e remoto, número de portas de conexão locais e remotas, estado da conexão, carimbo de data e hora da abertura da porta.

- O URL e o endereço IP da página da Web onde o conteúdo danoso ou suspeito foi detectado, o nome, tamanho e soma de verificação do arquivo que solicitou o URL, o identificador, peso e grau da regra utilizada para obter um veredito, o objetivo do ataque.

- Informações sobre as atualizações do aplicativo instalado e bancos de dados de antivírus: status de conclusão da tarefa de atualização, tipo de erro que pode ter ocorrido durante o processo de atualização, o número de atualizações sem êxito, o identificador do componente do aplicativo que executa as atualizações.

- Informações sobre o uso da Kaspersky Security Network (KSN): identificador da KSN, identificador do aplicativo, versão completa do aplicativo, endereço IP despersonalizado do dispositivo do usuário, indicadores da qualidade do cumprimento das solicitações da KSN, indicadores da qualidade do processamento de pacotes da KSN, indicadores do número de solicitações da KSN e informações sobre os tipos de solicitações da KSN, data e hora do início do envio das estatísticas, data e hora do término do envio das estatísticas, informações sobre as atualizações de configuração da KSN: identificador da configuração ativa, identificador da configuração recebida, código de erro da atualização da configuração.

- Informações sobre eventos de log do sistema: hora do evento, nome do registro onde o evento foi detectado, tipo e categoria do evento, nome da fonte do evento e descrição do evento.

- Informações para determinar a reputação de arquivos e endereços URL: o endereço de URL no qual a reputação está sendo solicitada e o Referenciador, o tipo de protocolo da conexão, o identificador interno do tipo de aplicativo, o número da porta que está sendo utilizada, o identificador de Usuário, a soma de verificação do arquivo verificado (MD5), tipo de ameaça detectada, informações sobre o registro usado para detectar uma ameaça (identificador de registro para os bancos de dados de antivírus, o registro de data e hora e o tipo); chave pública do certificado; impressão digital do certificado digital do objeto verificado e algoritmo de hash.

- Dados sobre a distribuição territorial do aplicativo: data de instalação e ativação do aplicativo, ID do parceiro que fornece a licença para a ativação do aplicativo, ID do aplicativo, ID de localização do idioma do aplicativo, número de série da licença para a ativação do aplicativo, sinal de participação da KSN.

- Informações sobre a licença usada: o tipo e o período de validade da licença, número de dias até a expiração da licença, identificador do parceiro de quem a licença foi adquirida, identificador do Centro de Ativação Regional, soma de verificação do código de ativação, hash do corpo do tíquete calculado usando o algoritmo SHA1, data e hora da criação do tíquete de licença, identificador de informações da licença, identificador do tíquete de licença, identificador da sequência do tíquete de licença, identificador exclusivo do computador do usuário, data a partir da qual o tíquete de licença começa a valer, data de expiração da validade do tíquete de licença, estado atual do tíquete de licença, versão do cabeçalho do tíquete, versão da licença, identificador do certificado de assinatura do cabeçalho do tíquete, soma de verificação do arquivo de chave, número de série do assinante do cabeçalho do tíquete, token de autenticação.

- Informações sobre o hardware instalado no computador: tipo, nome, nome do modelo, versão do firmware, parâmetros de dispositivos integrados e conectados.

- Informações sobre o dispositivo: ID do dispositivo.

- Informações sobre a operação do componente Controle da Web:
  versão do componente, motivo da categorização, informações adicionais sobre o motivo da categorização, URL categorizado, endereço IP do host do objeto bloqueado/categorizado.

Nota: dependendo das configurações do Kaspersky Security Center, é possível participar da Kaspersky Private Security Network, em vez da Kaspersky Security Network. O Kaspersky Endpoint Security envia uma notificação ao mudar da Kaspersky Private Security Network para a Kaspersky Security Network e solicita que você aceite os termos de Declaração da Kaspersky Security Network. Para obter informações detalhadas sobre a participação na Kaspersky Private Security Network, consulte a ajuda do Kaspersky Security Center.

Infraestrutura da Kaspersky Security Network

O Kaspersky Endpoint Security é compatível com as seguintes soluções de infraestrutura da Kaspersky Security Network:

- *KSN Global* é a solução usada pela maioria dos aplicativos da Kaspersky. Os participantes da KSN recebem informações da Kaspersky Security Network e enviam à Kaspersky informações sobre os objetos detectados no computador do usuário para serem analisados adicionalmente pelos analistas da Kaspersky e para serem incluídas nos bancos de dados de reputação e estatísticas da Kaspersky Security Network.

- *KSN Privada* é uma solução que permite aos usuários de computadores que hospedam o Kaspersky Endpoint Security ou outros aplicativos da Kaspersky obter acesso aos bancos de dados de reputação da Kaspersky Security Network e a outras estatísticas sem enviar dados para a Kaspersky Security Network de seus próprios computadores. A KSN Privada foi desenvolvida para clientes corporativos que não podem participar da Kaspersky Security Network por qualquer um dos seguintes motivos:

  - As estações de trabalho locais não estão conectadas à Internet.

  - A transmissão de quaisquer dados para fora do país ou fora da LAN corporativa é proibida por lei ou restrita pelas políticas de segurança corporativa.

Por padrão, o Kaspersky Security Center usa a KSN Global. Você pode configurar o uso da KSN Privada no Console de Administração do Kaspersky Security Center (MMC) e no Kaspersky Security Center Web Console. Não é possível configurar o uso da KSN Privada no Kaspersky Security Center Cloud Console.

Proxy da KSN

Os computadores gerenciados pelo Kaspersky Security Center Administration Server podem interagir com a Kaspersky Security Network por meio do serviço Proxy da KSN.

O serviço Proxy da KSN oferece os seguintes recursos:

- O computador do usuário pode consultar a KSN e enviar informações à KSN mesmo sem acesso direto à Internet.

- O serviço Proxy da KSN armazena em cache os dados processados, reduzindo assim a carga no canal de comunicação da rede externa e agilizando o recebimento das informações solicitadas pelo computador do usuário.

Para obter mais detalhes sobre o serviço de proxy da KSN, consulte a ajuda do Kaspersky Security Center.

Observação: A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinaturas de antimalware e atualizações de base de código), bem como a funcionalidade KSN, podem não estar disponíveis no software nos EUA.

Verifique a integridade dos componentes do aplicativo

O Kaspersky Endpoint Security contém vários módulos binários na forma de bibliotecas vinculadas dinâmicas, arquivos executáveis, arquivos de configuração e arquivos de interface. Os intrusos podem substituir um ou mais módulos de aplicativos executáveis ou arquivos por outros arquivos contendo código malicioso. Para evitar isso, o Kaspersky Endpoint Security pode verificar a integridade dos componentes do aplicativo. O aplicativo verifica módulos e arquivos quanto a alterações não autorizadas ou corrupção. Caso um módulo ou arquivo do aplicativo tenha uma soma de verificação incorreta, ele será considerado corrompido. O aplicativo verifica módulos e arquivos quanto a alterações não autorizadas ou corrupção. Caso um módulo ou arquivo do aplicativo tenha uma soma de verificação incorreta, ele será considerado corrompido.

A integridade dos componentes do aplicativo é verificada usando o utilitário integrity_checker localizado no diretório /Library/Application Support/Kaspersky Lab/KAV/Binaries directory. Esse utilitário verifica a integridade do arquivo manifesto que contém uma lista de arquivos do aplicativo cuja integridade é crítica para a operação correta do componente do aplicativo.

O arquivo manifesto integrity_check.xml, que é protegido pela assinatura criptográfica da Kaspersky, está localizado no mesmo diretório do utilitário integrity_checker (/Library/Application Support/Kaspersky Lab/KAV/Binaries).

Nota: os privilégios da conta de usuário raiz são necessários para executar o utilitário integrity_checker.

A verificação de integridade pode ser executada com o uso do utilitário instalado juntamente com o aplicativo ou com o uso do utilitário em um CD certificado.

Para verificar a integridade dos componentes do aplicativo, execute o seguinte comando:

```
sudo "/Library/Application Support/Kaspersky Lab/KAV/Binaries/integrity_checker"
```

Por padrão, o utilitário usa o arquivo integrity_check.xml localizado no diretório /Library/Application Support/Kaspersky Lab/KAV/Binaries.

Para exibir a ajuda dos ajustes do utilitário, execute o seguinte comando:

```
--help
```

O resultado da verificação de cada arquivo manifesto é exibido ao seu lado no seguinte formato:

- `SUCCEEDED` — a integridade dos arquivos está confirmada (código de retorno `0`)
- `FAILED` — a integridade dos arquivos não está confirmada (o código de retorno não é `0`)

Gerenciar o aplicativo por meio do Console de Administração do Kaspersky Security Center

O Kaspersky Security Center foi projetado para o gerenciamento centralizado da segurança da rede corporativa. Para obter informações detalhadas sobre o Kaspersky Security Center, consulte a ajuda do Kaspersky Security Center.

Também é possível gerenciar o Kaspersky Endpoint Security por meio da interface gráfica do usuário do aplicativo, no Web Console e Kaspersky Security Center Cloud Console e pela linha de comando.

Implantar o Kaspersky Endpoint Security em uma rede corporativa

1. Implantar o *Servidor de Administração* na rede.

   O Servidor de Administração é um componente do Kaspersky Security Center que armazena, de forma centralizada, informações sobre todos os aplicativos da Kaspersky instalados na rede corporativa para gerenciá-los.

2. Instale o *Console de Administração* na estação de trabalho do administrador do Kaspersky Security Center.

   O Console de Administração é um componente do Kaspersky Security Center que fornece uma interface do usuário para os serviços administrativos do Servidor de Administração e do *Agente de Rede*. O Agente de Rede coordena a interação entre o Servidor de Administração e o Kaspersky Endpoint Security instalado nos computadores da rede corporativa.

3. Instale o plugin de administração do Kaspersky Endpoint Security na estação de trabalho do administrador do Kaspersky Security Center.

   Um *plugin de administração* é um componente dedicado que fornece uma interface para gerenciar os aplicativos da Kaspersky por meio do Console de Administração. Cada aplicativo tem seu próprio plugin de administração. O plugin de administração é fornecido para todos os aplicativos da Kaspersky que podem ser gerenciados do Kaspersky Security Center.

4. Instale o Agente de Rede em computadores Mac remotos de uma das seguintes maneiras:

   - Localmente
   - Remotamente usando Apple Remote Desktop
   - Remotamente via Kaspersky Security Center
   - Remotamente usando o protocolo SSH

   Nota: para gerenciar o Kaspersky Endpoint Security for Mac 12.2.1 pelo Kaspersky Security Center, é necessário instalar o Agente de Rede versão 15 nos computadores remotos.

5. Instale o Kaspersky Endpoint Security em computadores Mac remotos de uma das seguintes maneiras:

   - Localmente
   - Remotamente usando Apple Remote Desktop
   - Remotamente usando o protocolo SSH
   - Remotamente via Kaspersky Security Center

   Importante: se o Kaspersky Internet Security for Mac ou um software antimalware de terceiros estiver instalado nos computadores remotos, desinstale-os antes de instalar o Kaspersky Endpoint Security.

Para obter informações detalhadas sobre como implantar o Servidor de Administração e instalar o Console de Administração, consulte a ajuda do Kaspersky Security Center.

Atualizar o Kaspersky Endpoint Security da versão 11.1 ou posterior para a versão 12.2.1

Nota: para gerenciar o Kaspersky Endpoint Security for Mac 12.2.1 pelo Kaspersky Security Center, é necessário instalar o Agente de Rede versão 15 nos computadores remotos.

É possível atualizar o Kaspersky Endpoint Security gerenciado pelo Kaspersky Security Center a partir da versão 11.1 ou posterior para a versão 12.2.1 em uma das seguintes maneiras:

- Atualize simultaneamente o Kaspersky Endpoint Security para a versão 12.2.1 e o Agente de Rede para a versão 15 nos computadores remotos.
- Primeiro, atualize o Agente de Rede para a versão 15 e depois o Kaspersky Endpoint Security para a versão 12.2.1.

Ao atualizar o aplicativo para uma versão mais recente, considere o seguinte:

- Para atualizar o Kaspersky Endpoint Security para a versão 12.2.1, é necessário o macOS 14 ou posterior.
- É necessário baixar o arquivo KES_11.3_profile.zip do site do Suporte Técnico para aplicar o novo perfil de configuração.
- Após atualizar o Kaspersky Endpoint Security para a versão 12.2.1, dois itens do Kaspersky Filter e dois do Kaspersky Monitor podem aparecer nas configurações de rede.
- Caso tenha o Kaspersky Endpoint Security versão 11.0.1 ou anterior, para atualizar o aplicativo para a versão 12.2.1, será necessário desinstalar o aplicativo e atualizar o macOS para a versão 14 ou posterior. Assim, será possível instalar o Kaspersky Endpoint Security versão 12.2.1.

Observação: A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinaturas de antimalware e atualizações de base de código), bem como a funcionalidade KSN, podem não estar disponíveis no software nos EUA.

Preparo para a instalação remota do Kaspersky Endpoint Security

Esta seção contém informações sobre a instalação do plugin de administração do Kaspersky Endpoint Security na estação de trabalho do administrador do Kaspersky Security Center e a instalação do Agente de Rede no computador remoto.

A instalação do plugin de administração do Kaspersky Endpoint Security e do Agente de Rede é um pré-requisito para a instalação do Kaspersky Endpoint Security via Kaspersky Security Center.

Instalar o plugin de administração do Kaspersky Endpoint Security

O plugin de administração do Kaspersky Endpoint Security fornece uma interface para gerenciar o Kaspersky Endpoint Security por meio do Console de Administração.

Instalar o plugin de administração do Kaspersky Endpoint Security

1. Na estação de trabalho do administrador do Kaspersky Security Center, descompacte o arquivo comprimido com os arquivos do pacote de instalação do Kaspersky Endpoint Security.
2. Abra a pasta com os arquivos do pacote de instalação do Kaspersky Endpoint Security.
3. Clique duas vezes em klcfginst.exe.

   A instalação do plugin de administração do Kaspersky Endpoint Security é iniciada.

Importante: antes de instalar o plugin de administração do Kaspersky Endpoint Security, feche o Console de Administração na estação de trabalho do administrador do Kaspersky Security Center.

Instalar o Agente de Rede localmente

O Agente de Rede coordena a interação entre o Servidor de Administração e o Kaspersky Endpoint Security instalado nos computadores da rede corporativa.

Instalar o Agente de Rede localmente

1. No computador remoto, abra a pasta com o kit de distribuição do Agente de Rede.
2. Abra o kit de distribuição do Agente de Rede (arquivo DMG).

   Uma janela com o conteúdo do kit de distribuição é aberta.
3. Na janela com o conteúdo do kit de distribuição, clique duas vezes em **Agente de Rede Kaspersky**.

4. Confirme que você deseja instalar o Agente de Rede clicando em **Continuar**.

5. Na janela **Introdução**, clique em **Continuar**.

6. Na janela **Licença**, leia o texto do Contrato de Licença de Usuário Final do Agente de Rede entre você e a AO Kaspersky Lab. Faça o seguinte:

   - Para aceitar todos os termos do contrato e prosseguir com a instalação, clique em **Continuar**.
   - Para imprimir o texto do contrato, clique em **Imprimir**.
   - Para salvar o contrato como um arquivo texto, clique em **Salvar**.

7. Na janela de confirmação, siga um destes procedimentos:

   - Para continuar com a instalação do Agente de Rede, clique em **Concordo**.
   - Para retornar ao texto do Contrato de Licença de Usuário Final, clique em **Ler licença**.
   - Para cancelar a instalação, clique em **Discordo**.

8. Na janela **Configurações**, faça o seguinte:

   a. No campo **Servidor**, especifique o Endereço IP ou o nome do DNS do servidor no qual o Kaspersky Security Center está instalado.

   b. No campo **Porta**, especifique o número da porta para uma conexão não criptografada com o servidor.

   c. No campo **Porta SSL**, especifique o número da porta para uma conexão SSL com o servidor.

   d. Se você deseja iniciar o Agente de Rede imediatamente após a instalação, marque a caixa de seleção **Executar após a instalação**.

   Se você não deseja usar o SSL para se conectar ao servidor, desmarque a caixa de seleção **Usar SSL**. Para continuar com a instalação, clique em **Continuar**.

9. Na janela **Tipo de instalação**, leia as informações sobre o disco no qual o Agente de Rede será instalado.

   Para instalar o Agente de Rede usando as configurações recomendadas, clique em **Instalar** e insira a senha de administrador para confirmar a escolha.

   Aguarde até o instalador do Agente de Rede conclua a instalação dos componentes do aplicativo.

10. Clique em **Fechar** para sair do instalador.

Instalar o Agente de Rede usando o Apple Remote Desktop

1. Em um computador remoto, escolha o **menu Apple** > **Ajuste do Sistema** > **Geral** > **Compartilhamento**.

2. Marque a caixa de seleção **Gerenciamento Remoto**.

3. Em outro Mac que será o servidor, instale o Apple Remote Desktop. Para obter mais informações sobre o Apple Remote Desktop, consulte o Suporte da Apple.

4. Abra o Apple Remote Desktop.

5. Na janela **Remote Desktop**, clique em **Verificador**, à esquerda, e selecione os dispositivos nos quais deseja instalar o Agente de Rede.

6. Clique em **Copiar**.

7. Clique em + e selecione os arquivos de instalação do Agente de Rede: os arquivos DMG, KUD e SH.

8. No menu pop-up **Colocar Itens Em**, escolha a **Pasta Superior do Disco**.

9. Clique em **Copiar**.

10. Depois que os arquivos forem copiados com sucesso, clique em **Unix**.

11. Digite o seguinte comando:

    ```
    cd /;
    ./install.sh --accept_eula -r <endereço do Servidor de Administração>
    ```

    onde `<endereço do Servidor de Administração>` é o nome DNS ou endereço IP do Servidor de Administração do Kaspersky Security Center.

    Nota: ao inserir esse comando, você aceita o Contrato de Licença de Usuário Final.

12. Escolha executar o comando como **Usuário** e digite “root” no campo.

13. Clique em **Enviar**.

A instalação do Agente de Rede será iniciada nos dispositivos selecionados.

Instalar o Agente de Rede usando o Kaspersky Security Center

O Kaspersky Security Center instala o Agente de Rede em um computador cliente usando uma conexão SSH.

Antes de instalar o Agente de Rede em um computador cliente, verifique se as seguintes condições foram atendidas:

- O Servidor de Administração do Kaspersky Security Center foi implantado na rede corporativa.
- O Console de Administração foi instalado na estação de trabalho do administrador do Kaspersky Security Center.
- O Login remoto foi ativado nos computadores remotos.
- Uma conta de administrador dedicada que será usada para executar a tarefa de instalação remota foi criada em um computador remoto. Você pode usar uma conta de domínio para a instalação.
- A senha do sudo foi desativada para a conta dedicada.

Criar um pacote de instalação do Agente de Rede

1. Inicie o Console de Administração do Kaspersky Security Center.

2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.

3. Na árvore do console, selecione a pasta **Avançado**, subpasta **Instalação remota** e então a subpasta **Pacotes de instalação**.

4. Na área de trabalho, clique em **Criar pacote de instalação**.

5. Na janela **Selecionar tipo de pacote de instalação**, clique em **Criar um pacote de instalação para um aplicativo da Kaspersky**.

6. Na janela **Definir o nome do pacote de instalação**, insira o nome do novo pacote de instalação no campo **Nome** e clique em **Avançar**.

7. Na janela **Selecionar o pacote de distribuição para instalação**, clique em **Procurar**.

   A janela para a seleção de um arquivo para criar o pacote de instalação é aberta.

8. Abra a pasta com o conteúdo do pacote de instalação do Agente de Rede e selecione o arquivo klnagent.kud.

   A janela **Selecionar o pacote de distribuição para instalação** exibe o nome e a versão do aplicativo a ser instalado remotamente usando o arquivo adicionado.

9. Clique em **Avançar**.

   O pacote de instalação do Kaspersky Endpoint Security é criado com as configurações especificadas.

10. Na última janela do assistente, clique em **Finalizar** para sair do assistente para novos pacotes.

Criar uma tarefa para instalação remota do Agente de Rede em um computador cliente

1. Inicie o Console de Administração do Kaspersky Security Center.

2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.

3. Selecione a pasta **Tarefas**.

4. Na área de trabalho, inicie o assistente para novas tarefas clicando em **Nova tarefa**.

5. Siga as etapas do Assistente para Novas Tarefas abaixo para criar uma tarefa para instalação remota do Kaspersky Endpoint Security no computador cliente.

Para prosseguir para a próxima etapa do assistente, clique em **Avançar**. Para retornar à etapa anterior do assistente, clique em ←. Para sair do assistente em qualquer etapa, clique em **Cancelar**.

Nota: a aparência dos botões pode variar dependendo da sua versão do Windows.

Etapa 1. Selecionar o tipo de tarefa

1. Na janela **Selecionar o tipo de tarefa**, maximize o nó do **Servidor de Administração do Kaspersky Security Center**.

2. Selecione a tarefa **Instalar o aplicativo remotamente**.

Etapa 2. Selecione o pacote de instalação

Na janela **Selecionar o pacote de instalação**, siga um destes procedimentos:

- Se o pacote de instalação do Agente de Rede com as configurações necessárias tiver sido criado anteriormente, selecione-o na lista de pacotes de instalação na parte superior da janela **Selecionar o pacote de instalação**.
- Caso o pacote de instalação necessário ainda não tenha sido criado, clique em **Novo** para iniciar o assistente para novos pacotes.

Etapa 3. Defina as configurações de instalação

Na janela **Configurações**, faça o seguinte:

1. Marque a caixa de seleção **Usando recursos do sistema operacional através do Servidor de Administração**.
2. Desmarque todas as outras caixas de seleção.

Etapa 4. Selecione um grupo de administração ao qual adicionar computadores após a instalação

Na janela **Mover para a lista de dispositivos gerenciados**, selecione um grupo para o qual os computadores serão movidos após a instalação, se necessário.

Etapa 5. Defina como selecionar os computadores clientes para os quais a tarefa será criada

Na janela **Selecionar os dispositivos aos quais a tarefa será atribuída**, selecione o método que deseja usar para especificar computadores clientes:

- Para selecionar entre os computadores detectados na rede pelo Servidor de Administração, selecione a opção **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**.
- Para especificar os endereços IP dos computadores manualmente ou importar os endereços IP dos computadores de um arquivo, selecione a opção **Especificar os endereços do dispositivo manualmente ou importar os endereços da lista**.
- Para criar uma tarefa para uma seleção de dispositivos com base em um critério predefinido, selecione a opção **Atribuir a tarefa a uma seleção de dispositivos**.
- Para selecionar computadores de um grupo de administração específico, selecione a opção **Atribuir uma tarefa à um grupo de administração**.

Etapa 6. Selecione os computadores clientes

Na janela que se abre (**Selecionar dispositivos**, **Seleção de dispositivos** ou **Selecionar grupo de Administração**, dependendo da opção selecionada na etapa anterior), selecione os computadores clientes, especifique os endereços IP dos computadores, especifique uma seleção de computadores ou selecione o grupo de administração ao qual a tarefa será aplicada.

Etapa 7. Selecione a conta para executar a tarefa

1. Na janela **Selecionar uma conta para executar a tarefa**, marque a caixa de seleção **Conta necessária (Agente de Rede não é usado)**.
2. Clique em **Adicionar** > **Conta**.

   A janela **Conta** é aberta.

3. Insira o login e a senha da conta de administrador dedicada de um computador remoto.

4. Clique em **OK**.

Etapa 8. Configure o agendamento de tarefas

1. Na janela **Configurar agendamento da tarefa**, selecione o modo de início na lista suspensa **Início agendado**.

2. Se necessário, configure uma tarefa agendada para iniciar automaticamente (especificando a data e hora de início da tarefa).

3. Se você deseja executar tarefas que o aplicativo não conseguiu iniciar de acordo com a programação (por exemplo, porque o computador foi desligado no horário agendado), marque a caixa de seleção **Executar tarefas ignoradas**.

   O Kaspersky Endpoint Security inicia a tarefa assim que o obstáculo que impede a inicialização da tarefa for eliminado.

Etapa 9. Especifique o nome da tarefa

Na janela **Definir o nome da tarefa**, digite o nome da tarefa que você está criando no campo **Nome**.

Etapa 10. Finalize a criação da tarefa

Na janela **Concluir a criação da tarefa**, faça o seguinte:

1. Se desejar que a tarefa seja iniciada assim que o assistente for concluído, marque a caixa de seleção **Executar tarefa após finalizar o Assistente**.

2. Clique em **Finalizar** para fechar o assistente.

Instalar o Agente de Rede usando o protocolo SSH

Uma maneira de instalar o Agente de Rede em um computador remoto é usando o protocolo SSH.

Verifique se os seguintes requisitos foram atendidos:

- O Servidor de Administração do Kaspersky Security Center foi implantado na rede corporativa.
- O Console de Administração foi instalado na estação de trabalho do administrador do Kaspersky Security Center.
- O pacote de instalação do Agente de Rede foi criado e armazenado em uma pasta compartilhada do Servidor de Administração.
- O Login remoto foi ativado no computador remoto.
- A conta do computador usada para instalar o Agente de Rede está incluída nos sudoers.

Para obter informações detalhadas sobre pacotes de instalação, consulte a ajuda do Kaspersky Security Center.

Instalar o Agente de Rede usando o protocolo SSH

1. Inicie o cliente SSH na estação de trabalho do administrador.

2. Conecte ao computador remoto.

3. Conecte a pasta compartilhada do Servidor de Administração como uma unidade de rede no computador remoto. Para fazer isso, digite os seguintes comandos no cliente SSH:

   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<conta do administrador>:<senha>@<endereço IP do Servidor de Administração>/KLSHARE /Volumes/KLSHARE
   ```

   Descrição dos parâmetros:

   - `<conta do administrador>` – Nome da conta de administrador no Servidor de Administração.
   - `<senha>` – Senha do administrador no Servidor de Administração.
   - `<endereço IP do Servidor de Administração>` – Endereço IP do servidor que hospeda o Kaspersky Security Center.

4. Execute o script de instalação. Para fazer isso, digite o seguinte comando no cliente SSH:

   ```
   cd /Volumes/KLSHARE/<pasta_do_pacote_klnagent>
   ```

   Em que `<pasta_do_pacote_klnagent>` é a pasta na qual o pacote de instalação do Agente de Rede está localizado.

   ```
   sudo ./install.sh --accept_eula [-r <servidor>] [-p <número da porta>] [-s use_ssl 0|1] [-l <número da porta SSL>] [-x use_proxy 0|1] [-a <proxy>] [-n <login de proxy>] [-w <senha de proxy>]
   ```

   Descrição dos parâmetros:

   - `<servidor>` – Endereço IP ou nome do DNS do servidor no qual o Kaspersky Security Center está instalado.
   - `<número da porta>` – Número da porta que será usada para estabelecer uma conexão não criptografada com o Servidor de Administração. A porta 14000 é usada por padrão.
   - `use_ssl 0|1` – Parâmetro que define se a criptografia será usada ao estabelecer a conexão entre o Agente de Rede e o Servidor de Administração. Se o valor for "0", uma conexão não criptografada será usada. Se o valor for "1", a conexão é estabelecida pelo protocolo SSL (valor padrão).
   - `<número da porta SSL>` – Número da porta que será usada para estabelecer uma conexão criptografada com o Servidor de Administração usando o protocolo SSL. A porta 13000 é usada por padrão.
   - `use_proxy 0|1` – parâmetro que define se um servidor proxy será usado ao se conectar à Internet. Se o valor for "0", um servidor proxy não será usado. Se o valor for "1", a conexão será estabelecida por meio do servidor proxy (o valor padrão).
   - `<proxy>` - Endereço IP ou nome DNS do servidor proxy.
   - `<proxy_login>` - Conta do usuário para conexão com o servidor proxy.
   - `<proxy_password>` - A senha para se conectar ao servidor proxy.

   Importante: é necessário ter direitos de administrador para executar este comando.

5. Desconecte a unidade de rede no computador remoto. Para fazer isso, digite o seguinte comando no cliente SSH:
   ```
   umount /Volumes/KLSHARE
   ```

6. Verifique se o Agente de Rede funciona corretamente no computador remoto. Para fazer isso, digite os seguintes comandos no cliente SSH:
   ```
   cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
   sudo ./klnagchk
   ```
   Se a verificação for bem-sucedida, o Agente de Rede funcionará corretamente.

Desinstalar o Agente de Rede localmente

1. No computador remoto, abra a pasta com o kit de distribuição do Agente de Rede.

2. Abra o kit de distribuição do Agente de Rede (arquivo DMG).
   Uma janela com o conteúdo do kit de distribuição é aberta.

3. Na janela com o conteúdo do kit de distribuição, clique duas vezes em **Desinstalador do Agente de Rede**.

4. Na janela **Introdução**, clique em **Continuar**.

5. Na janela **Informações**, clique em **Desinstalar**.

6. No prompt para as credenciais de administrador, insira um nome e uma senha de administrador e confirme que você deseja desinstalar o Agente de Rede.
   A desinstalação do Agente de Rede será iniciada.

7. Leia as informações sobre a desinstalação e clique em **Concluído** para sair do desinstalador.

O Agente de Rede foi removido do computador remoto.

Gerenciar o Agente de Rede a partir da linha de comando

Esta seção contém informações sobre como gerenciar o Agente de Rede usando a linha de comando em um computador cliente.

Você pode parar o Agente de Rede e reiniciá-lo usando a linha de comando em um computador cliente.

Você também pode conectar um computador remoto ao Servidor de Administração manualmente usando o utilitário klmover e verificar a conexão entre o computador remoto e o Servidor de Administração usando o utilitário klnagchk.

Você pode desinstalar o Agente de Rede.

Iniciar/parar o Agente de Rede em um computador remoto

Você pode parar o Agente de Rede e reiniciá-lo em um computador cliente usando a linha de comando.

Parar o Agente de Rede

No computador remoto, inicie o utilitário launchctl com o comando unload na linha de comando.

Sintaxe do comando:

```
sudo launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Iniciar o Agente de Rede

No computador remoto, inicie o utilitário launchctl com o comando load na linha de comando.

Sintaxe do comando:

```
sudo launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Importante: são necessários direitos de administrador para parar e iniciar o Agente de Rede.

Verificar a conexão entre um computador cliente e o Servidor de Administração manualmente. Utilitário Klnagchk

Verificar a conexão entre um computador remoto e o Servidor de Administração

No computador remoto, execute o utilitário klnagchk a partir da linha de comando.

O utilitário klnagchk está incluído no kit de distribuição do Agente de Rede.

Após a instalação do Agente de Rede, o utilitário klnagchk fica localizado na pasta /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Dependendo dos parâmetros especificados, o utilitário klnagchk executa as seguintes operações quando executado a partir da linha de comando:

- Exibe as configurações especificadas para a conexão entre o Agente de Rede instalado no computador remoto e o Servidor de Administração ou as salva em um arquivo.
- Salva as estatísticas do Agente de Rede (desde a última inicialização do Agente de Rede) e os resultados da execução do utilitário em um arquivo ou exibe essas informações na tela.
- Tenta estabelecer uma conexão entre o Agente de Rede e o Servidor de Administração.
- Se o utilitário não puder estabelecer uma conexão, ele envia um pacote ICMP para verificar o status do computador no qual o Servidor de Administração está instalado.

Antes de executar o utilitário, acesse /Library/Application Support/Kaspersky Lab/klnagent/Binaries na linha de comando.

Sintaxe do comando:

```
sudo ./klnagchk [-logfile <nome do arquivo>] [-sp] [-savecert <caminho do arquivo do certificado>] [-restart]
```

Importante: são necessários direitos de administrador para executar o utilitário.

Descrição dos parâmetros

`-logfile <nome do arquivo>` - Salva as configurações da conexão entre o Agente de Rede e o Servidor de Administração e os resultados da execução do utilitário em um arquivo. Se este parâmetro não for especificado, as configurações de conexão do servidor, os resultados da execução e as mensagens de erro serão exibidas na tela.

`-sp` – Exibe a senha para autenticação do servidor proxy na tela ou a salva em um arquivo. Este parâmetro é usado se o Agente de Rede se conectar ao Servidor de Administração por meio de um servidor proxy. Por padrão, este parâmetro não é usado.

`-savecert <nome do arquivo>` – Salva o certificado para autenticação no Servidor de Administração em um arquivo especificado.

`-restart` – Reinicia o Agente de Rede depois que o utilitário terminar a execução.

Exemplo:
sudo ./klnagchk -logfile klnagchk.log -sp

Conectar um computador remoto ao Servidor de Administração manualmente. Utilitário klmover

Conectar um computador remoto ao Servidor de Administração

No computador remoto, execute o utilitário klmover a partir da linha de comando.

O utilitário klmover está incluído no pacote de instalação do Agente de Rede.

Após a instalação do Agente de Rede, o utilitário klmover fica localizado na pasta /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Dependendo dos parâmetros especificados, o utilitário klmover executa as seguintes operações quando executado a partir da linha de comando:

- Conecta o Agente de Rede ao Servidor de Administração com os parâmetros especificados.
- Salva os resultados da execução do utilitário em um arquivo ou os exibe na tela.

Antes de executar o utilitário, acesse /Library/Application Support/Kaspersky Lab/klnagent/Binaries na linha de comando.

Sintaxe da linha de comando:

```
sudo ./klmover [-logfile <nome do arquivo>] [-address <endereço do servidor>] [-pn
<número da porta>] [-ps <número da porta SSL>] [-nossl] [-cert <caminho do arquivo do
certificado>] [-silent] [-dupfix]
```

Importante: são necessários direitos de administrador para executar o utilitário.

Descrição dos parâmetros

`-logfile <nome do arquivo>` – Salva os resultados da execução em um arquivo. Se este parâmetro não for especificado, os resultados da execução e as mensagens de erro serão exibidas na tela.

`-address <endereço do servidor>` – Endereço que o Agente de Rede usa para conectar ao Servidor de Administração. Você pode especificar o endereço IP ou o nome do DNS do servidor.

Nota: você também pode usar o comando com este parâmetro para alterar o endereço do Servidor de Administração ao qual os computadores remotos estão conectados.

`-pn <número da porta>` – Número da porta que será usada para estabelecer uma conexão não criptografada com o Servidor de Administração. A porta 14000 é usada por padrão.

`-ps <número da porta SSL>` – Número da porta que será usada para estabelecer uma conexão criptografada com o Servidor de Administração por meio do protocolo SSL. A porta 13000 é usada por padrão.

`-nossl` – Use uma conexão não criptografada com o Servidor de Administração. Se este parâmetro não for especificado, o Agente de Rede estabelecerá uma conexão segura com o Servidor de Administração por meio do protocolo SSL criptografado.

`-cert <caminho para arquivo do certificado>` – Use o arquivo de certificado especificado para autenticação em um novo Servidor de Administração. Se este parâmetro não for especificado, o Agente de Rede receberá um certificado na primeira conexão com o Servidor de Administração.

`-silent` – Execute o utilitário no modo silencioso.

`-dupfix` – Esse parâmetro é usado se o Agente de Rede tiver sido instalado de maneira diferente dos métodos descritos nesta ajuda, por exemplo, se tiver sido recuperado de uma imagem de disco com o Agente de Rede instalado. Se a autoidentificação automática do Agente de Rede resultar em ícones duplicados do computador original e de outros computadores no Console de Administração, tente reconectar os computadores duplicados.

Nota: ao executar o utilitário klmover, recomenda-se especificar valores para todos os parâmetros.

Exemplo:
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001

O computador remoto conectado ao Servidor de Administração via Agente de Rede é chamado *computador cliente*.

Desinstalar o Agente de Rede

Sintaxe do comando:

```
sudo '/Library/Application Support/Kaspersky Lab/klnagent/Binaries/UninstallScript'
```

Instalar e desinstalar o Kaspersky Endpoint Security

Esta seção descreve a instalação remota e a desinstalação do Kaspersky Endpoint Security em um computador cliente.

Também é possível instalar ou desinstalar o Kaspersky Endpoint Security localmente ou por meio do Kaspersky Security Center Web Console ou do Kaspersky Security Center Cloud Console.

Instalar o aplicativo usando o protocolo SSH

Antes de instalar o Kaspersky Endpoint Security em um computador remoto, verifique se as seguintes condições foram atendidas:

- O Servidor de Administração do Kaspersky Security Center foi implantado na rede corporativa.
- O Console de Administração foi instalado na estação de trabalho do administrador do Kaspersky Security Center.
- Um pacote de instalação do Kaspersky Endpoint Security foi criado e está localizado em uma pasta compartilhada no Servidor de Administração.
- Um arquivo de chave do Kaspersky Endpoint Security está armazenado na pasta compartilhada no Servidor de Administração (opcional).
- O Login remoto foi ativado no computador remoto.
- A conta do computador usada para instalar o aplicativo foi incluída nos sudoers.

Instalar o Kaspersky Endpoint Security em um computador cliente usando o protocolo SSH

1. Inicie o cliente SSH na estação de trabalho do administrador do Kaspersky Security Center.
2. Conecte ao computador remoto.
3. Conecte a pasta compartilhada do Servidor de Administração como uma unidade de rede no computador remoto. Para fazer isso, digite os seguintes comandos no cliente SSH:
   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<conta do administrador>:<senha>@<endereço IP do Servidor de
   Administração>/KLSHARE /Volumes/KLSHARE
   ```

Descrição dos parâmetros:

- `<conta do administrador>` – Nome da conta de administrador no Servidor de Administração.
- `<senha>` – Senha do administrador no Servidor de Administração.
- `<endereço IP do Servidor de Administração>` – Endereço IP do servidor que hospeda o Kaspersky Security Center.

4. Execute o script de instalação. Para fazer isso, digite os seguintes comandos no cliente SSH:

```
cd /Volumes/KLSHARE/<pasta do pacote KES>
./install.sh --accept_eula
```

em que `<pasta do pacote KES>` é a pasta na qual o pacote de instalação do Kaspersky Endpoint Security está localizado.

Importante: é necessário ter direitos de administrador para executar este comando.

5. Desconecte a unidade de rede no computador remoto. Para fazer isso, digite o seguinte comando no cliente SSH:

```
umount /Volumes/KLSHARE
```

Instalar o aplicativo usando o Kaspersky Security Center

Antes de instalar o Kaspersky Endpoint Security em um computador cliente, verifique se as seguintes condições foram atendidas:

- O Servidor de Administração do Kaspersky Security Center foi implantado na rede corporativa.
- O Console de Administração foi instalado na estação de trabalho do administrador do Kaspersky Security Center.
- O Agente de Rede foi instalado no computador cliente.
- Um pacote de instalação para o Kaspersky Endpoint Security foi criado e está armazenado na pasta compartilhada no Servidor de Administração.
- Um arquivo de chave do Kaspersky Endpoint Security está armazenado na pasta compartilhada no Servidor de Administração (opcional).
- O computador cliente foi adicionado ao grupo de administração de **Dispositivos gerenciados** no Servidor de Administração (opcional).

Para obter informações detalhadas sobre grupos de administração no Servidor de Administração, consulte a ajuda do Kaspersky Security Center.

Para instalar o Kaspersky Endpoint Security em um computador cliente usando o Kaspersky Security Center, você deve criar e iniciar a tarefa **Instalar o aplicativo remotamente**.

Criar uma tarefa para instalação remota do Kaspersky Endpoint Security em um computador cliente

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Selecione a pasta **Tarefas**.
4. Na área de trabalho, inicie o assistente para novas tarefas clicando em **Nova tarefa**.
5. Siga as etapas do Assistente para Novas Tarefas abaixo para criar uma tarefa para instalação remota do Kaspersky Endpoint Security no computador cliente.

Para prosseguir para a próxima etapa do assistente, clique em **Avançar**. Para retornar à etapa anterior do assistente, clique em ←. Para sair do assistente em qualquer etapa, clique em **Cancelar**.

Nota: a aparência dos botões pode variar dependendo da sua versão do Windows.

Etapa 1. Selecionar o tipo de tarefa

1. Na janela **Selecionar o tipo de tarefa**, maximize o nó do **Servidor de Administração do Kaspersky Security Center**.
2. Selecione a tarefa **Instalar o aplicativo remotamente**.

Etapa 2. Selecione o pacote de instalação

Na janela **Selecionar o pacote de instalação**, siga um destes procedimentos:

- Se o pacote de instalação do Kaspersky Endpoint Security com as configurações necessárias tiver sido criado anteriormente, selecione-o na lista de pacotes de instalação na parte superior da janela **Selecionar o pacote de instalação**.
- Caso o pacote de instalação necessário ainda não tenha sido criado, clique em **Novo** para iniciar o assistente para novos pacotes.

Etapa 3. Instale os aplicativos adicionais

Na janela **Avançado**, marque as caixas de seleção **Instalar o Agente de Rede junto com este aplicativo** e **<Nome do pacote de instalação do Agente de Rede>** se desejar instalar o Agente de Rede no computador cliente também.

Nota: o pacote de instalação do Agente de Rede deve ter sido criado anteriormente. Caso não tenha sido criado, clique em **Criar** para iniciar o assistente para novos pacotes.

Etapa 4. Defina as configurações de instalação

Na janela **Configurações**, configure a instalação remota do aplicativo.

Etapa 5. Selecione um grupo de administração ao qual adicionar computadores após a instalação

Na janela **Mover para a lista de dispositivos gerenciados**, selecione um grupo para o qual os computadores serão movidos após a instalação, se necessário.

Nota: a janela **Mover para a lista de dispositivos gerenciados** será exibida se você selecionar a instalação do Agente de Rede na etapa 3.

Etapa 6. Defina como selecionar os computadores clientes para os quais a tarefa será criada

Na janela **Selecionar os dispositivos aos quais a tarefa será atribuída**, selecione o método que deseja usar para especificar computadores clientes:

- Para selecionar entre os computadores detectados na rede pelo Servidor de Administração, selecione a opção **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**.
- Para especificar os endereços IP dos computadores manualmente ou importar os endereços IP dos computadores de um arquivo, selecione a opção **Especificar os endereços do dispositivo manualmente ou importar os endereços da lista**.
- Para criar uma tarefa para uma seleção de dispositivos com base em um critério predefinido, selecione a opção **Atribuir a tarefa a uma seleção de dispositivos**.
- Para selecionar computadores de um grupo de administração específico, selecione a opção **Atribuir uma tarefa à um grupo de administração**.

Etapa 7. Selecione os computadores clientes

Na janela que se abre (**Selecionar dispositivos**, **Seleção de dispositivos** ou **Selecionar grupo de Administração**, dependendo da opção selecionada na etapa anterior), selecione os computadores clientes, especifique os endereços IP dos computadores, especifique uma seleção de computadores ou selecione o grupo de administração ao qual a tarefa será aplicada.

Etapa 8. Selecione a conta para executar a tarefa

Na janela **Selecionar uma conta para executar a tarefa**, marque a caixa de seleção **Nenhuma conta necessária (Agente de Rede instalado)**.

Supõe-se que você instalou o Agente de Rede antes de iniciar este assistente.

Etapa 9. Configure o agendamento de tarefas

1. Na janela **Configurar agendamento da tarefa**, selecione o modo de início na lista suspensa **Início agendado**.
2. Se necessário, configure uma tarefa agendada para iniciar automaticamente (especificando a data e hora de início da tarefa).
3. Se você deseja executar tarefas que o aplicativo não conseguiu iniciar de acordo com a programação (por exemplo, porque o computador foi desligado no horário agendado), marque a caixa de seleção **Executar tarefas ignoradas**.

   O Kaspersky Endpoint Security inicia a tarefa assim que o obstáculo que impede a inicialização da tarefa for eliminado.

Etapa 10. Especifique o nome da tarefa

Na janela **Definir o nome da tarefa**, digite o nome da tarefa que você está criando no campo **Nome**.

Etapa 11. Finalize a criação da tarefa

Na janela **Concluir a criação da tarefa**, faça o seguinte:

1. Se desejar que a tarefa seja iniciada assim que o assistente for concluído, marque a caixa de seleção **Executar tarefa após finalizar o Assistente**.

2. Clique em **Finalizar** para fechar o assistente.

A tarefa que você criou aparece na área de trabalho da pasta **Tarefas**.

Criar um pacote de instalação

Ao criar a tarefa **Instalar aplicativo remotamente**, você pode usar um pacote de instalação existente ou criar um novo. Para visualizar a lista dos pacotes de instalação criados, clique em **Avançado** > **Instalação remota** > **Pacotes de instalação**.

Criar um pacote de instalação no Kaspersky Security Center

1. Inicie o Console de Administração do Kaspersky Security Center.

2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.

3. Na árvore do console, selecione a pasta **Avançado**, subpasta **Instalação remota** e então a subpasta **Pacotes de instalação**.

4. Na área de trabalho, clique em **Criar pacote de instalação**.

5. Na janela **Selecionar tipo de pacote de instalação**, clique em **Criar um pacote de instalação para um aplicativo da Kaspersky**.

6. Na janela **Definir o nome do pacote de instalação**, insira o nome do novo pacote de instalação no campo **Nome** e clique em **Avançar**.

7. Na janela **Selecionar o pacote de distribuição para instalação**, clique em **Procurar**.

   A janela para a seleção de um arquivo para criar o pacote de instalação é aberta.

8. Abra a pasta com o conteúdo do pacote de instalação do Kaspersky Endpoint Security e selecione o arquivo kesmac.kud.

   A janela **Selecionar o pacote de distribuição para instalação** exibe o nome e a versão do aplicativo a ser instalado remotamente usando o arquivo adicionado.

9. Marque a caixa de seleção **Copiar atualizações do repositório para o pacote de instalação** para copiar as atualizações do aplicativo do armazenamento do Kaspersky Security Center para o pacote de instalação, conforme necessário, e clique em **Avançar**.

   O pacote de instalação começa a ser carregado no Servidor de Administração. Quando o upload for concluído, a janela **Tipo de instalação** será aberta.

10. Na janela **Tipo de instalação**, na seção **Pacotes para instalar**, marque ou desmarque as caixas de seleção próximas aos nomes dos componentes que deseja ignorar durante a instalação no computador cliente e clique em **Próximo**.

    O pacote de instalação do Kaspersky Endpoint Security é criado com as configurações especificadas.

11. Na última janela do assistente, clique em **Finalizar** para concluir o assistente para novos pacotes.

Desinstalar o aplicativo usando o Kaspersky Security Center

Antes de remover o Kaspersky Endpoint Security de um computador cliente via Kaspersky Security Center, verifique se as seguintes condições foram atendidas:

- O Servidor de Administração do Kaspersky Security Center foi implantado na rede corporativa.
- O Console de Administração foi instalado na estação de trabalho do administrador do Kaspersky Security Center.
- O Agente de Rede foi instalado no computador cliente.

Para desinstalar o Kaspersky Endpoint Security do computador cliente via Kaspersky Security Center, você deve criar e iniciar a tarefa **Desinstalar o aplicativo remotamente**.

Importante: a remoção do Kaspersky Endpoint Security de um computador cliente pode representar um risco de infecção.

Criar uma tarefa para desinstalação remota do Kaspersky Endpoint Security de um computador cliente

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Selecione a pasta **Tarefas**.
4. Na área de trabalho, inicie o assistente para novas tarefas clicando em **Nova tarefa**.
5. Siga as etapas do Assistente para Novas Tarefas abaixo para criar uma tarefa de desinstalação remota do Kaspersky Endpoint Security a partir do computador cliente.

Para prosseguir para a próxima etapa do assistente, clique em **Avançar**. Para retornar à etapa anterior do assistente, clique em ←. Para sair do assistente em qualquer etapa, clique em **Cancelar**.

Nota: a aparência dos botões pode variar dependendo da sua versão do Windows.

Etapa 1. Selecionar o tipo de tarefa

1. Na janela **Selecionar o tipo de tarefa**, maximize o nó do **Servidor de Administração do Kaspersky Security Center**.
2. Expanda o nó filho **Avançado**.
3. Selecione a tarefa **Desinstalar o aplicativo remotamente**.

Etapa 2. Selecione o aplicativo para desinstalar

Na janela **Selecionar aplicativo a ser desinstalado**, selecione **Desinstalar o aplicativo compatível com o Kaspersky Security Center**.

Etapa 3. Definir configurações de desinstalação

Na janela **Configurações**, faça o seguinte:

1. Na lista suspensa **Aplicativo a ser desinstalado**, selecione **Kaspersky Endpoint Security for Mac 12.2.1**.
2. Clique em **Avançar**.
3. Configurar a desinstalação remota do aplicativo.

Etapa 4. Selecione a opção de reinicialização do sistema operacional

Na janela **Selecionando uma opção de reinício do sistema operacional**, selecione a opção **Não reiniciar o dispositivo**.

Etapa 5. Defina como selecionar os computadores clientes para os quais a tarefa será criada

Na janela **Selecionar os dispositivos aos quais a tarefa será atribuída**, selecione o método que deseja usar para especificar computadores clientes:

- Para selecionar entre os computadores detectados na rede pelo Servidor de Administração, selecione a opção **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**.
- Para especificar os endereços IP dos computadores manualmente ou importar os endereços IP dos computadores de um arquivo, selecione a opção **Especificar os endereços do dispositivo manualmente ou importar os endereços da lista**.
- Para criar uma tarefa para uma seleção de dispositivos com base em um critério predefinido, selecione a opção **Atribuir a tarefa a uma seleção de dispositivos**.
- Para selecionar computadores de um grupo de administração específico, selecione a opção **Atribuir uma tarefa à um grupo de administração**.

Etapa 6. Selecione os computadores clientes

Na janela que se abre (**Selecionar dispositivos**, **Seleção de dispositivos** ou **Selecionar grupo de Administração**, dependendo da opção selecionada na etapa anterior), selecione os computadores clientes, especifique os endereços IP dos computadores, especifique uma seleção de computadores ou selecione o grupo de administração ao qual a tarefa será aplicada.

Etapa 7. Selecione a conta para executar a tarefa

Na janela **Selecionar uma conta para executar a tarefa**, marque a caixa de seleção **Nenhuma conta necessária (Agente de Rede instalado)**.

Supõe-se que você instalou o Agente de Rede antes de iniciar este assistente.

Etapa 8. Configure o agendamento de tarefas

1. Na janela **Configurar agendamento da tarefa**, selecione o modo de início na lista suspensa **Início agendado**.
2. Se necessário, configure uma tarefa agendada para iniciar automaticamente (especificando a data e hora de início da tarefa).
3. Se você deseja executar tarefas que o aplicativo não conseguiu iniciar de acordo com a programação (por exemplo, porque o computador foi desligado no horário agendado), marque a caixa de seleção **Executar tarefas ignoradas**.

   O Kaspersky Endpoint Security inicia a tarefa assim que o obstáculo que impede a inicialização da tarefa for eliminado.

Etapa 9. Especifique o nome da tarefa

Na janela **Definir o nome da tarefa**, digite o nome da tarefa que você está criando no campo **Nome**.

Etapa 10. Finalize a criação da tarefa

Na janela **Concluir a criação da tarefa**, faça o seguinte:

1. Se desejar que a tarefa seja iniciada assim que o assistente for concluído, marque a caixa de seleção **Executar tarefa após finalizar o Assistente**.
2. Clique em **Finalizar** para fechar o assistente.

A tarefa que você criou aparece na área de trabalho da pasta **Tarefas**.

Iniciar e parar o aplicativo via Kaspersky Security Center

Você pode iniciar ou parar o Kaspersky Endpoint Security em um computador selecionado na lista de dispositivos gerenciados pelo Kaspersky Security Center.

Iniciar ou parar o Kaspersky Endpoint Security via Kaspersky Security Center

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Selecione o grupo de administração que contém o computador cliente necessário.
5. Selecione a guia **Dispositivos**.
6. Selecione o computador na lista de computadores clientes.
7. Abra a janela **Propriedades: <Nome do computador>** de uma das seguintes maneiras:
   - Clique duas vezes no nome do computador cliente.
   - Clique com o botão direito do mouse no computador cliente e escolha **Propriedades** a partir do menu de contexto.
8. Selecione a seção **Aplicativos**.
9. Na lista **Aplicativos da Kaspersky instalados no dispositivo**, clique com o botão direito do mouse para abrir o menu de contexto do item **Kaspersky Endpoint Security for Mac 12.2.1** e siga um destes procedimentos:
   - Para iniciar o aplicativo, selecione o item **Iniciar**.
   - Para parar o aplicativo, selecione o item **Parar**.

Importante: após a parada do Kaspersky Endpoint Security, o computador cliente continua funcionando no modo desprotegido, o que pode representar um risco de infecção.

Criar e gerenciar tarefas

Esta seção descreve como usar o Kaspersky Security Center para criar e configurar tarefas que o Kaspersky Endpoint Security executa em um computador cliente ou em um grupo de computadores.

Uma tarefa é um conjunto de ações configuráveis que o Kaspersky Endpoint Security executa em um computador cliente.

Você pode criar as seguintes tarefas no Kaspersky Security Center:

- Adicionar chave
- Verificação Rápida
- Reversão
- Verificação
- Atualização

Você pode executar as seguintes ações nas tarefas:

- Iniciar e parar tarefas.
- Definir configurações de tarefas.
- Rastrear o progresso de uma tarefa.
- Copiar e mover tarefas de um grupo para outro.
- Excluir tarefas.
- Importar e exportar tarefas.

Para mais informações sobre tarefas, consulte a ajuda do Kaspersky Security Center.

Criar tarefas

Ao gerenciar o Kaspersky Endpoint Security via Kaspersky Security Center, é possível criar os seguintes tipos de tarefas:

- Tarefas locais. *Uma tarefa local* é uma tarefa executada em um computador cliente separado.
- Tarefas de grupo. *Uma tarefa de grupo* é uma tarefa executada em computadores de um grupo de administração.
- Tarefas para um conjunto arbitrário de computadores. Você pode criar uma tarefa para ser executada em qualquer computador, independentemente de pertencerem a um grupo de administração ou a uma seleção de computador.

Criar uma tarefa local para um computador cliente separado

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Selecione o grupo de administração que contém o computador cliente necessário.
5. Na área de trabalho, selecione a guia **Dispositivos**.
6. Selecione o computador na lista de computadores clientes.
7. Abra a janela **Propriedades: <Nome do computador>** de uma das seguintes maneiras:
   - Clique duas vezes no nome do computador cliente.
   - Clique com o botão direito do mouse no computador cliente e escolha **Propriedades** a partir do menu de contexto.
8. Na janela **Propriedades: <Nome do computador>**, selecione a seção **Tarefas**.

   A lista de tarefas do sistema e tarefas personalizadas para o computador cliente selecionado é exibida na área de trabalho à direita.
9. Clique em **Adicionar** na parte inferior da área de trabalho.

   O Assistente para Novas Tarefas é iniciado.
10. Siga as etapas do Assistente para Novas Tarefas para criar uma tarefa local para um computador cliente separado.

Criar uma tarefa para computadores clientes em um grupo de administração

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Selecione o grupo de administração que contém o computador cliente necessário.
5. Na área de trabalho, selecione a guia **Tarefas**.
6. Na área de trabalho, inicie o assistente para novas tarefas clicando em **Nova tarefa**.
7. Siga as etapas do Assistente para Novas Tarefas para criar uma tarefa para computadores clientes incluídos no grupo de administração.

Para obter informações detalhadas sobre como criar tarefas de grupo, consulte a ajuda do Kaspersky Security Center.

Criar uma tarefa para um conjunto arbitrário de computadores

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Tarefas**.
4. Na área de trabalho, inicie o assistente para novas tarefas clicando em **Nova tarefa**.
5. Siga as etapas do Assistente para Novas Tarefas para criar uma tarefa para um conjunto arbitrário de computadores.

Para prosseguir para a próxima etapa do assistente, clique em **Avançar**. Para retornar à etapa anterior do assistente, clique em ←. Para sair do assistente em qualquer etapa, clique em **Cancelar**.

Nota: a aparência dos botões pode variar dependendo da sua versão do Windows.

Etapa 1. Selecionar um aplicativo e definir o tipo de tarefa

1. Na janela **Selecionar o tipo de tarefa**, maximize o nó do **Kaspersky Endpoint Security for Mac 12.2.1**.
2. Selecione o tipo da tarefa que deseja criar:
   - Para criar uma tarefa para adicionar uma chave, selecione **Adicionar chave**.
   - Para criar uma tarefa de verificação de áreas críticas, selecione **Verificação rápida**.
   - Para criar uma tarefa para reverter a atualização mais recente, selecione **Reversão**.
   - Para criar uma tarefa de verificação de vírus, selecione **Verificação**.
   - Para criar uma tarefa de atualização, selecione **Atualização**.

Etapa 2. Definir configurações para o tipo de tarefa selecionado

Dependendo do tipo de tarefa selecionado na etapa anterior, o conteúdo da janela de configurações pode variar. Esta janela não é exibida para a tarefa de reversão.

Ativação do aplicativo

Na janela **Ativação do aplicativo**, faça o seguinte:

1. Selecione um código ou chave de ativação no armazenamento do Kaspersky Security Center ou adicione um arquivo de chave armazenado no seu computador.
2. Para adicionar a chave especificada como chave reserva, marque a caixa de seleção **Adicionar uma chave reserva**.

   A chave reserva fica ativa quando a chave ativa atual expira.

As informações sobre a chave especificada (chave, tipo de chave e data de validade da chave) são exibidas na janela **Ativação do aplicativo**.

Atualização

Os servidores de atualização Kaspersky dedicados são a principal fonte de atualização do Kaspersky Endpoint Security. O Kaspersky Endpoint Security também pode usar pontos de distribuição, pastas locais ou outros servidores da Web como *fonte de atualização*.

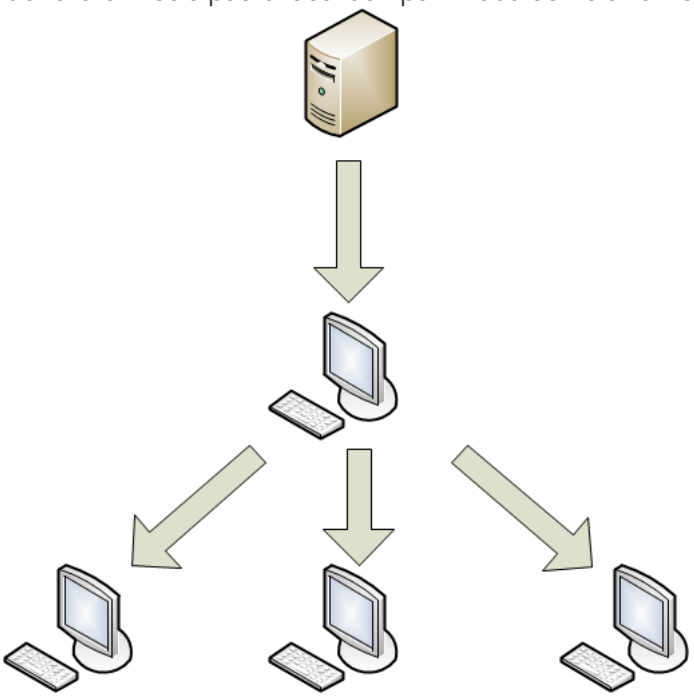
Você pode colocar as atualizações baixadas em uma pasta local para atualizar os bancos de dados do aplicativo e os módulos do Kaspersky Endpoint Security em outros computadores da rede corporativa para reduzir o tráfego da Internet.

Você pode configurar a distribuição de atualização da seguinte maneira:

1. Um dos computadores na rede recebe o pacote de atualização do Kaspersky Endpoint Security dos Servidores de atualização Kaspersky ou de uma fonte de atualização diferente. As atualizações recuperadas são colocadas em uma pasta local compartilhada.

   Nota: a pasta local compartilhada deve ser criada com antecedência.

2. Outros computadores na rede referem-se à pasta local compartilhada como a fonte de atualização.



Distribuição de atualizações por meio de um computador local

Se necessário, edite as configurações da Tarefa de atualização na janela **Atualização**:

1. Para desativar as atualizações dos módulos do aplicativo, desmarque a caixa de seleção **Atualizar módulos do aplicativo**.

2. Para alterar as fontes de atualização:

   a. Clique em **Configurações**.

      A janela **Configurações: Atualização** é aberta.

   b. Marque as caixas de seleção ao lado das fontes de atualização que deseja usar.

3. Para especificar uma fonte de atualização diferente, clique em **Adicionar**.

   A janela **Fonte de atualização** é aberta.

   a. Especifique o endereço da Web da fonte de atualização ou o caminho para uma pasta local ou de rede que seja uma fonte de atualização e clique em **OK**.

   b. Clique em **OK** para salvar as alterações e fechar a janela **Configurações: Atualização**.

Verificação e Verificação Rápida

Por padrão, o Kaspersky Endpoint Security usa o nível de segurança **Recomendado** e solicita uma ação do usuário ao detectar um objeto infectado após a verificação, verificando os seguintes objetos:

- Todas as unidades removíveis
- Todas as unidades internas
- Todas as unidades de rede
- Memória

> **Nota:** o Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.

Se necessário, edite as configurações de verificação na janela **Verificação**:

1. Selecione um dos níveis de segurança predefinidos ou personalize as configurações de segurança.
2. Especifique a ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto infectado.
3. Defina um escopo da verificação.

Etapa 3. Defina como selecionar os computadores clientes para os quais a tarefa será criada

> **Nota:** esta etapa não é relevante para tarefas locais ou de grupo.

Na janela **Selecionar os dispositivos aos quais a tarefa será atribuída**, selecione o método que deseja usar para especificar computadores clientes:

- Para selecionar entre os computadores detectados na rede pelo Servidor de Administração, selecione a opção **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**.
- Para especificar os endereços IP dos computadores manualmente ou importar os endereços IP dos computadores de um arquivo, selecione a opção **Especificar os endereços do dispositivo manualmente ou importar os endereços da lista**.

- Para criar uma tarefa para uma seleção de dispositivos com base em um critério predefinido, selecione a opção **Atribuir a tarefa a uma seleção de dispositivos**.
- Para selecionar computadores de um grupo de administração específico, selecione a opção **Atribuir uma tarefa à um grupo de administração**.

Etapa 4. Selecione os computadores clientes

Nota: esta etapa não é relevante para tarefas locais ou de grupo.

Na janela que se abre (**Selecionar dispositivos**, **Seleção de dispositivos** ou **Selecionar grupo de Administração**, dependendo da opção selecionada na etapa anterior), selecione os computadores clientes, especifique os endereços IP dos computadores, especifique uma seleção de computadores ou selecione o grupo de administração ao qual a tarefa será aplicada.

Etapa 5. Configure o agendamento de tarefas

1. Na janela **Configurar agendamento da tarefa**, selecione o modo de início na lista suspensa **Início agendado**.
2. Se necessário, configure uma tarefa agendada para iniciar automaticamente (especificando a data e hora de início da tarefa).
3. Se você deseja executar tarefas que o aplicativo não conseguiu iniciar de acordo com a programação (por exemplo, porque o computador foi desligado no horário agendado), marque a caixa de seleção **Executar tarefas ignoradas**.

   O Kaspersky Endpoint Security inicia a tarefa assim que o obstáculo que impede a inicialização da tarefa for eliminado.
4. Se desejar que o Kaspersky Security Center determine automaticamente o intervalo entre a inicialização da tarefa em computadores diferentes, marque a caixa de seleção **Usar atraso aleatório automaticamente para início das tarefas**.

   Isso ajuda a reduzir a carga no Servidor de Administração do Kaspersky Security Center.
5. Para definir manualmente o intervalo entre as inicializações de tarefas em computadores diferentes, marque a caixa de seleção **Usar atraso aleatório para inicialização de tarefas dentro de um intervalo de (min)** e especifique o número de minutos.

   Isso ajuda a reduzir a carga no Servidor de Administração do Kaspersky Security Center.

Etapa 6. Especifique o nome da tarefa

Na janela **Definir o nome da tarefa**, digite o nome da tarefa que você está criando no campo **Nome**.

Etapa 7. Finalize a criação da tarefa

Na janela **Concluir a criação da tarefa**, faça o seguinte:

1. Se desejar que a tarefa seja iniciada assim que o assistente for concluído, marque a caixa de seleção **Executar tarefa após finalizar o Assistente**.
2. Clique em **Finalizar** para fechar o assistente.

Iniciar e parar tarefas manualmente

As tarefas agendadas são iniciadas e paradas automaticamente de acordo com uma programação. No entanto, você pode iniciar uma tarefa manualmente a qualquer momento.

Nota: as tarefas são iniciadas em um computador cliente apenas se o Agente de Rede estiver em execução. Se a execução do Agente de Rede for interrompida, todas as tarefas ativas serão interrompidas.

Iniciar e parar tarefas manualmente

1. Abra a lista de tarefas que contém a tarefa que deseja iniciar ou parar.
2. Selecione a tarefa que deseja iniciar ou parar.
3. Inicie ou pare a tarefa de uma das seguintes maneiras:
   - Clique com o botão direito do mouse para exibir o menu de contexto da tarefa e escolha **Iniciar** ou **Parar**.
   - Na área de trabalho, clique em **Iniciar** ou **Parar**.
   - Clique com o botão direito do mouse para exibir o menu de contexto da tarefa e escolha **Propriedades**. Na janela exibida, clique em **Iniciar** ou **Parar**.

Tarefas de importação e exportação

Você pode exportar tarefas de grupo e tarefas de um conjunto arbitrário de computadores para um arquivo.

Exportar uma tarefa

1. Selecione a lista de tarefas da qual deseja exportar a tarefa:
   - Selecione o grupo de administração e abra a guia **Tarefas**.
   - Na árvore do console, clique em **Tarefas**.
2. Clique com o botão direito do mouse na tarefa que deseja exportar e, no menu de atalho da tarefa, escolha **Todas as tarefas** > **Exportar**.
3. Na janela **Salvar como**, especifique o nome do arquivo e o local em que a tarefa exportada será salva.
4. Clique em **Salvar**.

Importar uma tarefa

1. Selecione a lista de tarefas para a qual deseja importar a tarefa:
   - Selecione o grupo de administração e abra a guia **Tarefas**.
   - Na árvore do console, clique em **Tarefas**.

2. Importe a tarefa de qualquer uma das seguintes maneiras:

   - No menu de atalho da lista de tarefas, selecione **Todas as tarefas** > **Importar**.
   - Clique em **Importar tarefa de um arquivo**.

3. Na janela **Abrir**, especifique o caminho para o arquivo da tarefa que deseja importar.
4. Clique em **Abrir**.

   A tarefa é exibida na lista de tarefas.

Exibir tarefas

Você pode exibir a lista de tarefas criadas para um computador específico, para computadores em um grupo de administração específico ou a lista de todas as tarefas não locais.

Exibir tarefas para um grupo de administração específico

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Selecione o grupo de administração que contém o computador cliente necessário.
5. Na área de trabalho, selecione a guia **Tarefas**.

   A lista de tarefas para os computadores no grupo de administração selecionado é exibida.

Exibir tarefas locais

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Selecione o grupo de administração que contém o computador cliente necessário.
5. Na área de trabalho, selecione a guia **Dispositivos**.
6. Selecione o computador na lista de computadores clientes.
7. Abra a janela **Propriedades: <Nome do computador>** de uma das seguintes maneiras:

   - Clique duas vezes no nome do computador cliente.
   - Clique com o botão direito do mouse no computador cliente e escolha **Propriedades** a partir do menu de contexto.

8. Na janela **Propriedades: <Nome do computador>**, selecione a seção **Tarefas**.

A lista de tarefas do sistema e tarefas personalizadas para o computador cliente selecionado é exibida na área de trabalho à direita.

Exibir tarefas não locais

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Tarefas**.

A lista de tarefas não locais criadas para computadores que podem ou não fazer parte de grupos de administração é exibida.

Gerenciar configurações específicas da tarefa

Exibir configurações de uma tarefa local

1. Abra a lista de tarefas locais.
2. Selecione uma tarefa na lista e abra as configurações da tarefa de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa.
   - Clique com o botão direito do mouse para exibir o menu de atalho da tarefa e selecione **Propriedades**.

Exibir configurações de uma tarefa de grupo

1. Abra a lista de tarefas de grupo para um grupo de administração.
2. Selecione uma tarefa na lista e abra as configurações da tarefa de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa.
   - Clique com o botão direito do mouse para exibir o menu de atalho da tarefa e selecione **Propriedades**.
   - Clique no link **Configurar a tarefa** na área de trabalho.

Exibir configurações de uma tarefa não local

1. Abra a lista de tarefas não locais.
2. Selecione uma tarefa na lista e abra as configurações da tarefa de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa.
   - Clique com o botão direito do mouse para exibir o menu de atalho da tarefa e selecione **Propriedades**.
   - Clique no link **Configurar a tarefa** na área de trabalho.

Para mais informações sobre tarefas, consulte a ajuda do Kaspersky Security Center.

Para tarefas locais, tarefas de grupo ou tarefas para um conjunto arbitrário de computadores

Definir as configurações da tarefa Adicionar chave

1. Abra a janela com as configurações da Tarefa **Adicionar chave**.
2. Selecione a seção **Ativação do aplicativo**.
3. Se necessário, adicione outra chave de uma das seguintes maneiras:
   - Para selecionar uma chave ou um código de ativação entre os códigos de ativação adicionados ao armazenamento do Kaspersky Security Center:
     a. Selecione a opção **Chave ou código de ativação**.
     b. Clique em **Procurar**.
        A janela **Chaves e códigos de ativação no armazenamento do Kaspersky Security Center** é aberta.
     c. Selecione uma chave ou código de ativação.
     d. Clique em **OK**.
   - Para adicionar um arquivo de chave:
     a. Selecione a opção **Arquivo de chave**.
     b. Clique em **Adicionar**.
        A janela de seleção de arquivo é aberta.
     c. Selecione um arquivo de chave.
     d. Clique em **Abrir**.

   Nota: a chave atual é excluída quando uma chave diferente é adicionada.

4. Para adicionar a chave especificada como chave reserva, marque a caixa de seleção **Adicionar uma chave reserva**.
   A chave reserva fica ativa quando a chave atual expira.

   Nota: a data de expiração da chave reserva deve ser posterior à data de expiração atual da chave.

5. Salve as alterações de uma das seguintes maneiras:
   - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da tarefa>** após salvar as alterações.
   - Clique em **OK** para fechar a janela **Propriedades: <Nome da tarefa>** após salvar as alterações.

Gerenciar as configurações da tarefa de Verificação Rápida

1. Abra a janela com as configurações da tarefa de **Verificação rápida**.
2. Selecione a seção **Verificação Rápida**.
3. Para alterar o nível de segurança em que o Kaspersky Endpoint Security executa a Tarefa de verificação rápida, siga um destes procedimentos na seção **Nível de segurança**:

   - Selecione um nível de segurança predefinido movendo o controle deslizante para cima ou para baixo na escala.

     Você pode selecionar um dos seguintes níveis de segurança:

     - **Proteção máxima**. O Kaspersky Endpoint Security realiza o monitoramento máximo de arquivos abertos, salvos ou executados.
     - **Recomendado**. O Kaspersky Endpoint Security monitora os arquivos com as configurações recomendadas pela Kaspersky.

       Esse é o nível de segurança padrão.
     - **Velocidade máxima**. O Kaspersky Endpoint Security monitora um conjunto mínimo de arquivos. Você pode escolher esse nível de segurança se quiser usar outros aplicativos que exijam recursos significativos de memória.

   - Definir as configurações de segurança manualmente:

     a. Clique em **Configurações**.

        A janela **Configurações: Verificação** é aberta.

     b. Na guia **Geral**, na seção **Tipos de arquivos**, selecione os tipos de arquivos que devem ser verificados pelo Kaspersky Endpoint Security ao executar a Tarefa de verificação rápida.

     c. Na guia **Geral**, na seção **Otimização**, defina as configurações de desempenho da verificação.

     d. Na guia **Geral**, na seção **Arquivos compostos**, selecione os arquivos compostos a serem analisados pelo Kaspersky Endpoint Security quanto a objetos detectáveis.

     e. Na guia **Avançado**, na seção **Configurações avançadas**, configure o uso da tecnologia iSwift e o salvamento de informações sobre objetos detectados nas estatísticas do aplicativo.

     f. Na guia **Avançado**, na seção **Analisador heurístico**, configure o uso do Analisador heurístico e selecione o nível de proteção a ser aplicado por ele durante as verificações de malware.

     g. Clique em **OK** para salvar as alterações e fechar a janela **Configurações: Verificação**.

        O nível de segurança é alterado para **Personalizado**.

   - Para restaurar as configurações padrão, clique em **Padrão**.

     O nível de segurança é alterado para **Recomendado**.

4. Se necessário, na seção **Ação**, selecione a ação que o Kaspersky Endpoint Security deve executar quando um objeto infectado for detectado.

5. Para especificar um escopo da verificação, na seção **Escopo da verificação**, clique em Configurações e faça o seguinte na janela **Escopo da verificação** que se abre:

   a. Se desejar que o Kaspersky Endpoint Security verifique a memória do computador, marque a caixa de seleção **Memória**.

   b. Se desejar que o Kaspersky Endpoint Security verifique os objetos de inicialização, marque a caixa de seleção **Itens de início**.

   c. Se desejar que o Kaspersky Endpoint Security verifique outros arquivos ou pastas adicionais, clique em **Adicionar** e especifique um arquivo, pasta ou máscara para nomes de arquivos ou pastas.

   d. Clique em **OK** para salvar as alterações e fechar a janela **Escopo da verificação**.

6. Salve as alterações de uma das seguintes maneiras:

   - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da tarefa>** após salvar as alterações.
   - Clique em **OK** para fechar a janela **Propriedades: <Nome da tarefa>** após salvar as alterações.

Definir as configurações da tarefa de Verificação

1. Abra a janela com as configurações da tarefa de **Verificação**.
2. Selecione a seção **Verificação**.
3. Para alterar o nível de segurança em que o Kaspersky Endpoint Security executa a Tarefa de verificação, siga um destes procedimentos na seção **Nível de segurança**:

   - Selecione um nível de segurança predefinido movendo o controle deslizante para cima ou para baixo na escala.

     Você pode selecionar um dos seguintes níveis de segurança:

     - **Proteção máxima**. O Kaspersky Endpoint Security realiza o monitoramento máximo de arquivos abertos, salvos ou executados.
     - **Recomendado**. O Kaspersky Endpoint Security monitora os arquivos com as configurações recomendadas pela Kaspersky.

       Esse é o nível de segurança padrão.
     - **Velocidade máxima**. O Kaspersky Endpoint Security monitora um conjunto mínimo de arquivos. Você pode escolher esse nível de segurança se quiser usar outros aplicativos que exijam recursos significativos de memória.

   - Definir as configurações de segurança manualmente:

     a. Clique em **Configurações**.

        A janela **Configurações: Verificação** é aberta.

     b. Na guia **Geral**, na seção **Tipos de arquivos**, selecione os tipos de arquivos que devem ser verificados pelo Kaspersky Endpoint Security ao executar a Tarefa de verificação.

     c. Na guia **Geral**, na seção **Otimização**, defina as configurações de desempenho da verificação.

d. Na guia **Geral**, na seção **Arquivos compostos**, selecione os arquivos compostos a serem analisados pelo Kaspersky Endpoint Security quanto a objetos detectáveis.

e. Na guia **Avançado**, na seção **Configurações avançadas**, configure o uso da tecnologia iSwift e o salvamento de informações sobre objetos detectados nas estatísticas do aplicativo.

f. Na guia **Avançado**, na seção **Analisador heurístico**, configure o uso do Analisador heurístico e selecione o nível de proteção a ser aplicado por ele durante as verificações de malware.

g. Clique em **OK** para salvar as alterações e fechar a janela **Configurações: Verificação**.

O nível de segurança é alterado para **Personalizado**.

- Para restaurar as configurações padrão, clique em **Padrão**.

  O nível de segurança é alterado para **Recomendado**.

4. Se necessário, na seção **Ação**, selecione a ação que o Kaspersky Endpoint Security deve executar quando um objeto infectado for detectado.

5. Para especificar um escopo da verificação, na seção **Escopo da verificação**, clique em Configurações e faça o seguinte na janela **Escopo da verificação** que se abre:

   a. Se desejar que o Kaspersky Endpoint Security verifique todas as unidades removíveis, marque a caixa de seleção **Todos os discos removíveis**.

   b. Se desejar que o Kaspersky Endpoint Security verifique todas as unidades internas, marque a caixa de seleção **Todos os discos internos**.

   c. Se desejar que o Kaspersky Endpoint Security verifique todas as unidades de rede, marque a caixa de seleção **Todos os discos de rede**.

   d. Se desejar que o Kaspersky Endpoint Security verifique a memória do computador, marque a caixa de seleção **Memória**.

   e. Se desejar que o Kaspersky Endpoint Security verifique os objetos de inicialização, marque a caixa de seleção **Itens de início**.

   f. Se desejar que o Kaspersky Endpoint Security verifique outros arquivos ou pastas, clique em **Adicionar** e especifique um arquivo, pasta ou máscara para nomes de arquivos ou pastas.

   g. Clique em **OK** para salvar as alterações e fechar a janela **Escopo da verificação**.

6. Salve as alterações de uma das seguintes maneiras:

   - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da tarefa>** após salvar as alterações.
   - Clique em **OK** para fechar a janela **Propriedades: <Nome da tarefa>** após salvar as alterações.

Gerenciar as configurações da tarefa de atualização

1. Abra a janela com as configurações da tarefa de **Atualização**.

2. Selecione a seção **Atualização**.

3. Se desejar que o Kaspersky Endpoint Security atualize os módulos do aplicativo junto com os bancos de dados do aplicativo, marque a caixa de seleção **Atualizar módulos do aplicativo**.

4. Para escolher uma fonte de atualização:

   a. Clique em **Configurações**.

      A janela **Configurações: Atualização** é aberta.

   b. Especifique a fonte de atualização de uma das seguintes maneiras:

      - Se desejar que o aplicativo baixe atualizações do Servidor de Administração, marque a caixa de seleção **Kaspersky Security Center**.
      - Se quiser que o aplicativo baixe atualizações dos Servidores de atualização Kaspersky, marque a caixa de seleção **Servidores de atualização Kaspersky**.
      - Para adicionar uma fonte de atualização diferente, clique em **Adicionar** e, na janela exibida, insira o caminho para a fonte de atualização.

        Por padrão, o Kaspersky Endpoint Security baixa atualizações dos Servidores de atualização Kaspersky.

   c. Clique em **OK** para salvar as alterações e fechar a janela **Configurações: Atualização**.

5. Salve as alterações de uma das seguintes maneiras:

   - Clique em **Aplicar** para permanecer na janela **Propriedades: <Nome da tarefa>** após salvar as alterações.
   - Clique em **OK** para fechar a janela **Propriedades: <Nome da tarefa>** após salvar as alterações.

Apenas para tarefas locais

Gerenciar as configurações da tarefa de Proteção Contra Ameaças ao Arquivo

1. Abra a lista de tarefas locais para um computador cliente.
2. Na lista de tarefas locais, selecione a tarefa Proteção Contra Ameaças ao Arquivo e abra suas propriedades de uma das seguintes maneiras:

   - Clique duas vezes no nome da tarefa.
   - Clique com o botão direito do mouse para exibir o menu de atalho da tarefa e selecione **Propriedades**.
   - Clique em **Propriedades**.

3. Selecione a seção **Proteção Contra Ameaças ao Arquivo**.
4. Se necessário, defina as seguintes configurações:

   - Ative ou desative a Proteção Contra Ameaças ao Arquivo no computador cliente.
   - Para selecionar um dos níveis de segurança predefinidos, use o controle deslizante na seção **Nível de segurança**.

- Para definir as configurações de segurança manualmente, clique em **Configurações** e, na janela **Configurações: Proteção Contra Ameaças ao Arquivo** que se abre, faça o seguinte:

  a. Na guia **Geral**, na seção **Tipos de arquivos**, selecione os tipos de arquivos que o Kaspersky Endpoint Security deve verificar quando forem abertos, executados ou salvos.

  b. Na guia **Geral**, na seção **Otimização**, defina as configurações de desempenho da verificação, selecione a tecnologia de verificação e selecione se o Kaspersky Endpoint Security ignorará a verificação de volumes de sistema somente leitura em computadores cliente.

  c. Na guia **Geral**, na seção **Arquivos compostos**, selecione quais arquivos compostos devem ser verificados quanto a objetos detectáveis e defina uma restrição para a verificação de objetos grandes.

  d. Na guia **Escopo da proteção**, especifique os arquivos ou as pastas que devem ser verificados pela Proteção Contra Ameaças ao Arquivo.

  Por padrão, todos os objetos localizados em unidades removíveis, internas e unidades de rede conectadas ao computador cliente são verificadas. É possível adicionar um objeto ao escopo de proteção, modificar um objeto na lista, desativar temporariamente a verificação de um objeto na lista ou remover um objeto da lista.

  e. Na guia **Avançado**, na seção **Modo de verificação**, selecione o modo de Proteção Contra Ameaças ao Arquivo.

  f. Na guia **Avançado**, na seção **Pausar tarefa**, ative ou desative a pausa agendada da Proteção Contra Ameaças ao Arquivo e configure a pausa automática de tarefas de acordo com uma programação.

  g. Na guia **Avançado**, na seção **Analisador heurístico**, configure o uso do Analisador heurístico pela Proteção Contra Ameaças ao Arquivo.

  h. Clique em **OK** para salvar as alterações e fechar a janela **Configurações: Proteção Contra Ameaças ao Arquivo**.

- Na seção **Se um objeto malicioso for detectado**, selecione a ação que a Proteção Contra Ameaças ao Arquivo deve executar ao detectar um objeto infectado.

5. Salve as alterações de uma das seguintes maneiras:

   - Clique em **Aplicar** para permanecer na janela **Propriedades: Proteção Contra Ameaças ao Arquivo** após salvar as alterações.

   - Clique em **OK** para fechar a janela **Propriedades: Proteção Contra Ameaças ao Arquivo** após salvar as alterações.

Gerenciar as configurações da tarefa Proteção Contra Ameaças da Web

1. Abra a lista de tarefas locais para um computador cliente.

2. Na lista de tarefas locais, selecione a tarefa Proteção Contra Ameaças da Web e abra suas propriedades de uma das seguintes maneiras:

   - Clique duas vezes no nome da tarefa.

   - Clique com o botão direito do mouse para exibir o menu de atalho da tarefa e selecione **Propriedades**.

   - Clique em **Propriedades**.

3. Selecione a seção **Proteção Contra Ameaças da Web**.

4. Se necessário, defina as seguintes configurações:

   - Ative ou desative a Proteção Contra Ameaças da Web no computador cliente.

   - Para selecionar um dos níveis de segurança predefinidos, use o controle deslizante na seção **Nível de segurança**.

   - Para definir as configurações de segurança manualmente, clique em **Configurações** e, na janela **Configurações: Proteção Contra Ameaças da Web** que se abre, faça o seguinte:

     a. Na guia **Geral**, na seção **Modo de verificação**, ative ou desative a verificação de endereços da Web no banco de dados de endereços da Web maliciosos.

     b. Na guia **Geral**, na seção **Configurações antiphishing**, ative ou desative a verificação de endereços da Web no banco de dados de endereços da Web de phishing.

     c. Na guia **Geral**, na seção **Configurações antiphishing**, ative ou desative o uso do Analisador heurístico para detectar links de phishing.

     d. Na guia **Endereços da Web confiáveis**, ative ou desative a verificação de tráfego da web de endereços da web confiáveis e crie ou edite uma lista de endereços da web confiáveis.

     e. Clique em **OK** para salvar as alterações e fechar a janela **Configurações: Proteção Contra Ameaças da Web**.

5. Na seção **Se um objeto malicioso for detectado**, selecione a ação que a Proteção contra ameaças da Web executa ao detectar um objeto perigoso no tráfego da Web.

6. Salve as alterações de uma das seguintes maneiras:

   - Clique em **Aplicar** para permanecer na janela **Propriedades: Proteção Contra Ameaças da Web** após salvar as alterações.

   - Clique em **OK** para fechar a janela **Propriedades: Proteção Contra Ameaças da Web** após salvar as alterações.

Gerenciar as configurações da tarefa de Verificação Rápida

1. Abra a lista de tarefas locais para um computador cliente.

2. Na lista de tarefas locais, selecione a tarefa de Verificação Rápida e abra suas propriedades de uma das seguintes maneiras:

   - Clique duas vezes no nome da tarefa.

   - Clique com o botão direito do mouse para exibir o menu de atalho da tarefa e selecione **Propriedades**.

   - Clique em **Propriedades**.

3. Selecione a seção **Verificação**.

4. Se necessário, defina as seguintes configurações:

   - Para selecionar um dos níveis de segurança predefinidos, use o controle deslizante na seção **Nível de segurança**.

   - Para definir as configurações de segurança manualmente, clique em **Configurações** e, na janela **Configurações: Verificação** que se abre, faça o seguinte:

     a. Na guia **Geral**, na seção **Tipos de arquivos**, selecione os tipos de arquivos que devem ser verificados pelo Kaspersky Endpoint Security.

     b. Na guia **Geral**, na seção **Otimização**, defina as configurações de desempenho da verificação.

     c. Na guia **Geral**, na seção **Arquivos compostos**, selecione os arquivos compostos que você deseja que o Kaspersky Endpoint Security verifique.

     d. Na guia **Avançado**, na seção **Configurações avançadas**, configure o uso da tecnologia iSwift e o salvamento de informações sobre objetos detectados nas estatísticas do aplicativo.

     e. Na guia **Avançado**, na seção **Analisador heurístico**, configure o uso do Analisador heurístico e selecione o nível de proteção a ser aplicado por ele.

     f. Clique em **OK** para salvar as alterações e fechar a janela **Configurações: Verificação**.

   - Na seção **Ação**, selecione a ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto infectado.

   - Para especificar um escopo da verificação, na seção **Escopo da verificação**, clique em Configurações e faça o seguinte na janela **Escopo da verificação** que se abre:

     - Se você deseja que o Kaspersky Endpoint Security verifique objetos na lista padrão, marque a caixa de seleção ao lado do objeto relevante.

     - Se desejar que o Kaspersky Endpoint Security verifique outros arquivos ou pastas, clique em **Adicionar** e especifique um arquivo, pasta ou máscara para nomes de arquivos ou pastas.

     - Clique em **OK** para salvar as alterações e fechar a janela **Escopo da verificação**.

5. Salve as alterações de uma das seguintes maneiras:

   - Clique em **Aplicar** para permanecer na janela **Propriedades: Verificação Rápida** após salvar as alterações.

   - Clique em **OK** para fechar a janela **Propriedades: Verificação Rápida** após salvar as alterações.

Gerenciar as configurações da tarefa de Verificação Completa

1. Abra a lista de tarefas locais para um computador cliente.

2. Na lista de tarefas locais, selecione a tarefa de Verificação Completa e abra suas propriedades de uma das seguintes maneiras:

   - Clique duas vezes no nome da tarefa.

   - Clique com o botão direito do mouse para exibir o menu de atalho da tarefa e selecione **Propriedades**.

   - Clique em **Propriedades**.

3. Selecione a seção **Verificação**.

4. Se necessário, defina as seguintes configurações:

- Para selecionar um dos níveis de segurança predefinidos, use o controle deslizante na seção **Nível de segurança**.
- Para definir as configurações de segurança manualmente, clique em **Configurações** e, na janela **Configurações: Verificação** que se abre, faça o seguinte:

  a. Na guia **Geral**, na seção **Tipos de arquivos**, selecione os tipos de arquivos que devem ser verificados pelo Kaspersky Endpoint Security.

  b. Na guia **Geral**, na seção **Otimização**, defina as configurações de desempenho da verificação.

  c. Na guia **Geral**, na seção **Arquivos compostos**, selecione os arquivos compostos que você deseja que o Kaspersky Endpoint Security verifique.

  d. Na guia **Avançado**, na seção **Configurações avançadas**, configure o uso da tecnologia iSwift e o salvamento de informações sobre objetos detectados nas estatísticas do aplicativo.

  e. Na guia **Avançado**, na seção **Analisador heurístico**, configure o uso do Analisador heurístico e selecione o nível de proteção a ser aplicado por ele.

  f. Clique em **OK** para salvar as alterações e fechar a janela **Configurações: Verificação**.

- Na seção **Ação**, selecione a ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto infectado.
- Para especificar um escopo da verificação, na seção **Escopo da verificação**, clique em Configurações e faça o seguinte na janela **Escopo da verificação** que se abre:

  - Se você deseja que o Kaspersky Endpoint Security verifique objetos na lista padrão, marque a caixa de seleção ao lado do objeto relevante.
  - Se desejar que o Kaspersky Endpoint Security verifique outros arquivos ou pastas, clique em **Adicionar** e especifique um arquivo, pasta ou máscara para nomes de arquivos ou pastas.
  - Clique em **OK** para salvar as alterações e fechar a janela **Escopo da verificação**.

5. Salve as alterações de uma das seguintes maneiras:

- Clique em **Aplicar** para permanecer na janela **Propriedades: Verificação Completa** após salvar as alterações.
- Clique em **OK** para fechar a janela **Propriedades: Verificação Completa** após salvar as alterações.

Gerenciar as configurações da tarefa de Verificação Personalizada

1. Abra a lista de tarefas locais para um computador cliente.
2. Na lista de tarefas locais, selecione a tarefa de Verificação Personalizada e abra suas propriedades de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa.
   - Clique com o botão direito do mouse para exibir o menu de atalho da tarefa e selecione **Propriedades**.
   - Clique em **Propriedades**.
3. Selecione a seção **Verificação**.
4. Se necessário, defina as seguintes configurações:
   - Para selecionar um dos níveis de segurança predefinidos, use o controle deslizante na seção **Nível de segurança**.
   - Para definir as configurações de segurança manualmente, clique em **Configurações** e, na janela **Configurações: Verificação** que se abre, faça o seguinte:
     a. Na guia **Geral**, na seção **Tipos de arquivos**, selecione os tipos de arquivos que devem ser verificados pelo Kaspersky Endpoint Security.
     b. Na guia **Geral**, na seção **Otimização**, defina as configurações de desempenho da verificação.
     c. Na guia **Geral**, na seção **Arquivos compostos**, selecione os arquivos compostos que você deseja que o Kaspersky Endpoint Security verifique.
     d. Na guia **Avançado**, na seção **Configurações avançadas**, configure o uso da tecnologia iSwift e o salvamento de informações sobre objetos detectados nas estatísticas do aplicativo.
     e. Na guia **Avançado**, na seção **Analisador heurístico**, configure o uso do Analisador heurístico e selecione o nível de proteção a ser aplicado por ele.
     f. Clique em **OK** para salvar as alterações e fechar a janela **Configurações: Verificação**.
   - Na seção **Ação**, selecione a ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto infectado.
   - Para especificar um escopo da verificação, na seção **Escopo da verificação**, clique em Configurações e faça o seguinte na janela **Escopo da verificação** que se abre:
     - Clique em **Adicionar** e especifique um arquivo, pasta ou máscara de nome de um arquivo ou pasta.
     - Clique em **OK** para salvar as alterações e fechar a janela **Escopo da verificação**.
5. Salve as alterações de uma das seguintes maneiras:
   - Clique em **Aplicar** para permanecer na janela **Propriedades: Verificação Personalizada** após salvar as alterações.
   - Clique em **OK** para fechar a janela **Propriedades: Verificação Personalizada** após salvar as alterações.

Gerenciar as configurações da tarefa Proteção Contra Ameaças à Rede

1. Abra a lista de tarefas locais para um computador cliente.
2. Na lista de tarefas locais, selecione a tarefa Proteção Contra Ameaças à Rede e abra suas propriedades de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa.
   - Clique com o botão direito do mouse para exibir o menu de atalho da tarefa e selecione **Propriedades**.
   - Clique em **Propriedades**.
3. Selecione a seção **Proteção Contra Ameaças à Rede**.
4. Se necessário, defina as seguintes configurações:
   - Ative ou desative a Proteção Contra Ameaças à Rede no computador cliente.
   - Na seção **Configurações de Proteção Contra Ameaças à Rede**, marque ou desmarque a caixa de seleção **Bloquear computadores responsáveis pelo ataque** pelo **<valor> min** e especifique o valor.
   - Você também pode especificar os endereços IP dos computadores cuja atividade de rede não será bloqueada. Para isso, execute as seguintes etapas:
     a. Clique em **Exclusões**.
        A janela **Exclusões** é aberta.
     b. Clique em **Adicionar**.
        A janela **Endereço IP** é aberta.
     c. Especifique o Endereço IP do computador cuja atividade de rede não será bloqueada e clique em **OK**.
     d. Clique em **OK** para salvar as alterações e fechar a janela **Exclusões**.
5. Salve as alterações de uma das seguintes maneiras:
   - Clique em **Aplicar** para permanecer na janela **Propriedades: Proteção Contra Ameaças à Rede** após salvar as alterações.
   - Clique em **OK** para fechar a janela **Propriedades: Proteção Contra Ameaças à Rede** após salvar as alterações.

Criar e gerenciar políticas

Esta seção contém informações sobre como criar e configurar políticas para o Kaspersky Endpoint Security.

Uma política determina as configurações de um aplicativo e gerencia a capacidade de configurar esse aplicativo em dispositivos dentro de um grupo de administração. Uma política individual deve ser criada para cada aplicativo. É possível criar um número ilimitado de políticas para aplicativos instalados em dispositivos em cada grupo de administração, mas apenas uma política pode ser aplicada a cada aplicativo por vez em um grupo de administração.

Nota: ao criar e configurar uma política, você pode permitir ou proibir alterações em qualquer grupo de configurações nas políticas usando os botões e .

Você pode executar as seguintes ações em políticas personalizadas:

- Criar políticas.
- Configurar políticas.
- Copiar ou mover políticas de um grupo para outro.
- Excluir políticas.
- Alterar o status de políticas.
- Exportar políticas para um arquivo.
- Importar políticas de um arquivo.

Para obter informações detalhadas sobre as políticas do Kaspersky Security Center, consulte a ajuda do Kaspersky Security Center.

Criar uma política

Esta seção contém instruções sobre como iniciar o Assistente para Novas Políticas para criar uma política.

Criar uma política a partir da pasta de um grupo de administração

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Selecione o grupo de administração que contém o computador cliente necessário.
5. Na área de trabalho, selecione a guia **Políticas** e clique em **Nova política**.
   O Assistente para Novas Políticas é aberto.
6. Siga as etapas do Assistente para Novas Políticas para criar uma política.

Criar uma política a partir da pasta Políticas

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.

3. Na árvore do console, clique em **Políticas**.

4. Na área de trabalho, clique em **Nova política**.

   O Assistente para Novas Políticas é aberto.

5. Siga as etapas do Assistente para Novas Políticas para criar uma política.

Para prosseguir para a próxima etapa do assistente, clique em **Avançar**. Para retornar à etapa anterior do assistente, clique em ←. Para sair do assistente em qualquer etapa, clique em **Cancelar**.

Nota: a aparência dos botões pode variar dependendo da sua versão do Windows.

Etapa 1. Selecione um aplicativo

Na janela **Selecione o aplicativo para o qual deseja criar uma política de grupo**, na lista de aplicativos, selecione **Kaspersky Endpoint Security for Mac (12.2.1)**.

Etapa 2. Especifique o nome da política

1. Na janela **Inserir um nome de política de grupo**, no campo **Nome**, especifique o nome da política que está criando. O nome não pode conter os seguintes símbolos: " * < : > ? \ |.

2. Marque a caixa de seleção **Usar as configurações de política para uma versão anterior do aplicativo** se desejar importar as configurações de uma política existente do Kaspersky Endpoint Security para uma nova política.

Etapa 3. Especifique as configurações de proteção

Na janela **Proteção**, defina as seguintes configurações, se necessário:

- Defina as configurações de proteção para o sistema operacional no computador cliente.
- Configure a zona confiável.

  É possível criar uma lista de objetos que não são verificados ou monitorados pelo Kaspersky Endpoint Security.
- Configure os aplicativos confiáveis.

  É possível criar uma lista de aplicativos cuja atividade de rede e de arquivos não será monitorada pelo Kaspersky Endpoint Security.
- Selecione os tipos de objetos a serem detectados.
- Desative ou ative a inicialização de tarefas agendadas quando o computador estiver funcionando com bateria.
- Limitar o uso da CPU pelas tarefas de verificação.

Etapa 4. Defina as configurações da Proteção Contra Ameaças ao Arquivo

Na janela **Proteção Contra Ameaças ao Arquivo**, faça o seguinte, se necessário:

- Ative/desative a Proteção Contra Ameaças ao Arquivo.

  Por padrão, a Proteção Contra Ameaças ao Arquivo está ativada.
- Selecione um nível de segurança.

  Por padrão, o nível de segurança recomendado pela Kaspersky está selecionado.

- Definir as configurações de Proteção Contra Ameaças ao Arquivo.
- Selecione a ação a ser executada ao detectar um objeto malicioso.

Etapa 5. Defina as configurações da Proteção Contra Ameaças da Web

Na janela **Proteção Contra Ameaças da Web**, faça o seguinte, se necessário:

- Ative/desative a Proteção Contra Ameaças da Web.
  Por padrão, a Proteção Contra Ameaças da Web é ativada.
- Selecione um nível de segurança.
  Por padrão, o nível de segurança recomendado pela Kaspersky está selecionado.
- Definir as configurações de Proteção Contra Ameaças da Web.
- Selecione a ação a ser executada ao detectar um objeto malicioso no tráfego da Web.

Etapa 6. Defina as configurações da Proteção Contra Ameaças à Rede

Na janela **Proteção Contra Ameaças à Rede**, faça o seguinte, se necessário:

- Ative/desative a Proteção Contra Ameaças à Rede.
  Por padrão, a Proteção Contra Ameaças à Rede está ativada.
- Defina as configurações da Proteção Contra Ameaças à Rede.
- Crie ou edite uma lista de endereços IP de computadores remotos cujas atividades de rede nunca serão bloqueadas pelo Kaspersky Endpoint Security.

Etapa 7. Definir as configurações de atualização

Na janela **Atualização**, faça o seguinte, se necessário:

- Ative ou desative a atualização dos módulos do aplicativo.
- Especifique fontes de atualização.

Etapa 8. Defina as configurações da KSN

Na janela **Kaspersky Security Network**, faça o seguinte, se necessário:

- Leia o texto completo da Declaração da Kaspersky Security Network, clicando em **Declaração da KSN**.
- Visualizar informações sobre a infraestrutura da KSN fornecidas pelo Kaspersky Security Center.
- Ative ou desative o uso da Kaspersky Security Network.
- Ative ou desative o modo KSN estendido.
- Ative ou desative o uso de um proxy da KSN.
- Ative ou desative o uso dos servidores da Kaspersky quando o proxy da KSN estiver indisponível.

Nota: o uso da Kaspersky Security Network e de um proxy da KSN em computadores remotos estará disponível apenas se o Servidor de Administração do Kaspersky Security Center for usado como servidor proxy. Para obter informações detalhadas sobre as propriedades do Servidor de Administração, consulte a ajuda do Kaspersky Security Center.

Se a infraestrutura da KSN Global for usada pelo Kaspersky Security Center e você optar por participar da Kaspersky Security Network nas configurações da política, as estatísticas do Kaspersky Endpoint Security dos computadores clientes aos quais a política é aplicada serão enviadas automaticamente para a Kaspersky para aprimorar a proteção desses computadores.

Nota: a Kaspersky não recebe, processa ou armazena nenhum dado pessoal sem o seu consentimento explícito.

Dados fornecidos à Kaspersky ao usar a Kaspersky Security Network na infraestrutura da KSN Global

Se a caixa de seleção **Concordo em usar a Kaspersky Security Network** estiver marcada e a caixa de seleção **Ativar modo KSN estendido** estiver desmarcada, o Kaspersky Endpoint Security fornece à Kaspersky os seguintes dados:

- Informações sobre a licença usada: o tipo e o período de validade da licença, número de dias até a expiração da licença, identificador do parceiro de quem a licença foi adquirida, identificador do Centro de Ativação Regional, soma de verificação do código de ativação, hash do corpo do tíquete calculado usando o algoritmo SHA1, data e hora da criação do tíquete de licença, identificador de informações da licença, identificador do tíquete de licença, identificador da sequência do tíquete de licença, identificador exclusivo do computador do usuário, data a partir da qual o tíquete de licença começa a valer, data de expiração da validade do tíquete de licença, estado atual do tíquete de licença, versão do cabeçalho do tíquete, versão da licença, identificador do certificado de assinatura do cabeçalho do tíquete, soma de verificação do arquivo de chave, número de série do assinante do cabeçalho do tíquete, token de autenticação.

- Versão completa do software instalado;
  tipo do Software instalado;
  ID de atualização do Software; ID do serviço de reputação; ID do tipo de protocolo; ID de um centro de ativação regional; versão da lista de decisões revogadas do serviço de Software; ID do registro acionado nos bancos de dados de antivírus do Software; carimbo de data e hora do registro acionado nos bancos de dados de antivírus do Software; tipo do registro acionado nos bancos de dados de antivírus do Software; ID exclusiva da instância da instalação do aplicativo no computador; data de ativação da licença; data de expiração da licença; identificador da licença; status da licença usada pelo Software; tipo de soma de verificação do objeto que está sendo processado; nome do malware detectado ou do software legítimo que pode ser usado para causar danos ao dispositivo ou aos dados do usuário; soma de verificação do objeto que está sendo processado; soma de verificação do código de ativação do Software; versão completa do Software; ID exclusivo do dispositivo; ID do Software; soma de verificação do arquivo da chave do Software; ID do modelo de informações usado para fornecer a licença do Software; identificador do certificado usado para assinar o cabeçalho do tíquete de licença do Software; data e hora de criação do tíquete de licença do Software; a soma de verificação do tíquete de licença do Software; a versão do tíquete de licença do Software; a versão do código de ativação do Software; formato dos dados na solicitação para a infraestrutura do Titular dos Direitos; ID do tíquete de licença atual; o ID de componente do Software; o resultado da ação do Software; código de erro; endereço acessado do serviço Web (URL, IP); número da porta; endereço web da origem da solicitação de serviço da web (referenciador); chave pública do certificado; impressão digital do certificado digital do objeto verificado e algoritmo de hash.

Se as caixas de seleção **Concordo em usar a Kaspersky Security Network** e **Ativar modo KSN estendido** estiverem marcadas, o Kaspersky Endpoint Security fornecerá à Kaspersky os seguintes dados:

- Informações sobre a versão do sistema operacional (SO) e os service packs instalados no computador, a versão e as somas de verificação (MD5, SHA2-256, SHA1) do arquivo de kernel do SO, parâmetros do modo de execução do SO; versão do SO, número da compilação do SO, número da atualização do SO, edição do SO, informações estendidas sobre a edição do SO; versão do Service Pack do SO; data e hora da inicialização do SO; tempo de atraso do processamento do evento sobre a ação do SO no subsistema de análise comportamental; número de eventos da ação atrasada do SO do tipo atual; tempo de atraso de processamento do evento sobre a ação do SO no subsistema de defesa proativo; número de eventos processadas de ação do SO; número de eventos da ação processada síncrona do SO; atraso total de todos os eventos da ação do SO do tipo atual; tempo de atraso de processamento do evento sobre a ação do SO no subsistema de armazenamento de eventos persistentes; atraso total de todos os eventos da ação do SO; número de eventos da ação em espera síncrona do SO; data e hora do evento recebido de uma ação no SO.

- Informações sobre a última reinicialização do SO com falha: número de reinicializações com falha.

- Informações sobre o aplicativo instalado do Titular dos direitos e o status da proteção antivírus: ID de instalação do Software (PCID); Versão do registro do banco de dados do software; identificados exclusivo da instância da instalação do aplicativo no computador, tipo do aplicativo, ID do tipo do aplicativo, a versão completa do aplicativo instalado, a versão do identificador das configurações do aplicativo, o identificador do tipo de computador, o identificador exclusivo do computador em que o aplicativo está instalado, o identificador exclusivo do Usuário nos serviços do Titular de Direitos, idioma local e estado da operação, versão dos componentes do Software instalado e seus estados de operação, versão do protocolo usado para conectar com os serviços do Titular de Direitos; versão completa do software instalado; tipo do Software instalado; ID de atualização do Software; ID do serviço de reputação; ID do tipo de protocolo; ID de um centro de ativação regional; versão da lista de decisões revogadas do serviço de Software; ID do registro acionado nos bancos de dados de antivírus do Software; carimbo de data e hora do registro acionado nos bancos de dados de antivírus do Software; tipo do registro acionado nos bancos de dados de antivírus do Software; ID exclusiva da instância da instalação do aplicativo no computador; data de ativação da licença; data de expiração da licença; identificador da licença; status da licença usada pelo Software; tipo de soma de verificação do objeto que está sendo processado; nome do malware detectado ou do software legítimo que pode ser usado para causar danos ao dispositivo ou aos dados do usuário; soma de verificação do objeto que está sendo processado; soma de verificação do código de ativação do Software; versão completa do Software; ID do Software; soma de verificação do arquivo da chave do Software; ID do modelo de informações usado para fornecer a licença do Software; identificador do certificado usado para assinar o cabeçalho do tíquete de licença do Software; data e hora de criação do tíquete de licença do Software; a soma de verificação do tíquete de licença do Software; a versão do tíquete de licença do Software; a versão do código de ativação do Software; formato dos dados na solicitação para a infraestrutura do Titular dos Direitos; ID do tíquete de licença atual; o ID de componente do Software; o resultado da ação do Software; código de erro; endereço acessado do serviço Web (URL, IP); número da porta; endereço web da origem da solicitação de serviço da web (referenciador); número de ciclos atualização-aplicação para bases de dados antivírus; data e hora em que as bases de dados de antivírus foram atualizadas e aplicadas pela última vez; data e hora do lançamento nos bancos de dados do Software; versão do componente do Software; ID de atualização do Software; tipo do Software instalado; data e hora da inicialização do Inspetor do Sistema; data e hora da instalação do Software; probabilidade de enviar estatísticas pelo Inspetor do Sistema; código do evento que demorou mais tempo do que o tempo padrão a processar pelo Inspetor do Sistema; tempo de processamento da base de dados do evento que demorou mais tempo do que o tempo padrão a processar pelo Inspetor do Sistema; tempo máximo permitido para processamento de um evento pelo Inspetor do Sistema; tempo de processamento do evento que levou mais tempo do que o padrão para ser processado pelo Inspetor do Sistema; número total de eventos que demoraram mais tempo do que o tempo padrão para processar pelo Inspetor do Sistema.

- Informações sobre todos os objetos e operações processados: Veredito do software sobre o objeto sendo processado; código do diretório; tamanho do objeto que está sendo processado; soma de verificação (SHA256) do objeto que está sendo processado; número do software detectado no contexto do Inspetor do Sistema; data e hora da detecção do software pelo Inspetor do Sistema; detectar características; ID do registro acionado nos bancos de dados de antivírus do Software; motivo da detecção do software pelo Inspetor do Sistema; soma de verificação (MD5) do objeto que está sendo processado; resultado da verificação de integridade do módulo; nome do objeto que está sendo processado; tipo do registro acionado nos bancos de dados de antivírus do Software; caminho para o objeto que está sendo processado; o nome do objeto verificado; a data e hora da verificação; os endereços URL e de referência dos quais foi baixado; o tamanho dos arquivos verificados e os caminhos para eles; o sinal de arquivo; a data e hora da criação do arquivo; o nome, tamanho e somas de verificação (MD5, SHA2-256) do compactador (se o arquivo foi empacotado); a entropia do arquivo; o tipo de arquivo; o código do tipo de arquivo; o sinal, ID e formato do arquivo executável; a soma de verificação do objeto (MD5, SHA2-256); o tipo e o valor da soma de verificação suplementar do objeto; dados sobre a assinatura digital do objeto (certificado): dados sobre o editor do certificado, número de inicializações do objeto desde a última entrega de estatísticas, ID da tarefa de verificação do aplicativo, meio de recebimento de informações sobre a reputação do objeto, valor do filtro alvo, parâmetros técnicos das tecnologias de detecção aplicáveis; caminho para o objeto que está sendo processado; código do diretório.

- Para arquivos executáveis: a entropia das seções do arquivo, indicador de verificação de reputação ou indicador de assinatura de arquivo, nome, tipo, tipo de ID, soma de verificação (MD5) e o tamanho do aplicativo que foi carregado pelo objeto que está sendo validado, o caminho do aplicativo e os caminhos do modelo, um atributo indicando presença na lista de Autorun, data de entrada, lista de atributos, nome do compactador, informações sobre a assinatura digital do aplicativo: o certificado do editor, o nome do arquivo carregado no formato MIME, a data e hora de compilação do arquivo.

- Informações sobre aplicativos iniciados e os seus módulos: somas de verificação (MD5, SHA2-256) de arquivos em execução, tamanho, atributos, data de criação, nome do compactador (se o arquivo foi compactado), nomes de arquivos, informações sobre processos em execução no sistema (ID do processo (PID)), nome do processo, informações sobre a conta a partir da qual o processo foi iniciado, o aplicativo e o comando que iniciaram o processo, o caminho completo para os arquivos do processo e a linha de comando inicial, uma descrição do aplicativo ao qual o processo pertence (o nome do aplicativo e as informações sobre o editor, além dos certificados digitais usados e as informações necessárias para verificar a autenticidade ou as informações sobre a ausência de assinatura digital de um arquivo), e informações sobre os módulos carregados nos processos: seus nomes, tamanhos, tipos, datas de criação, atributos, somas de verificação (MD5, SHA2-256, SHA1), os caminhos para eles, informações do cabeçalho do arquivo PE, nomes dos compactadores (se o arquivo foi compactado), informações sobre a disponibilidade e validade dessas estatísticas, identificador do modo para gerar as estatísticas que estão sendo enviadas.

- Se forem detectadas ameaças ou vulnerabilidades, além das informações sobre o objeto detectado, são fornecidas informações sobre o identificador, a versão e o tipo do registro no banco de dados de antivírus, o nome da ameaça com base na classificação da Kaspersky, a data e hora da última atualização do banco de dados de antivírus, o nome do arquivo executável, a soma de verificação (MD5) do arquivo do aplicativo que solicitou o URL no qual a ameaça foi detectada, o endereço IP (IPv4 ou IPv6) da ameaça detectada, o identificador de vulnerabilidade e seu nível de ameaça, o URL e o referenciador da página da Web em que a vulnerabilidade foi detectada.

- Se um objeto potencialmente malicioso for detectado, são fornecidas informações sobre os dados na memória dos processos.

- Informações sobre ataque de rede: endereço IP do computador atacante e número da porta no computador do usuário visado pelo ataque de rede, ID do protocolo de ataque, nome e tipo de ataque.

- Informações sobre conexões de rede: versão e somas de verificação (MD5, SHA2-256, SHA1) do arquivo a partir do qual foi iniciado o processo que abriu a porta, caminho para o arquivo do processo e a respectiva assinatura digital, endereços IP local e remoto, número de portas de conexão locais e remotas, estado da conexão, carimbo de data e hora da abertura da porta.

- O URL e o endereço IP da página da Web onde o conteúdo danoso ou suspeito foi detectado, o nome, tamanho e soma de verificação do arquivo que solicitou o URL, o identificador, peso e grau da regra utilizada para obter um veredito, o objetivo do ataque.

- Informações sobre as atualizações do aplicativo instalado e bancos de dados de antivírus: status de conclusão da tarefa de atualização, tipo de erro que pode ter ocorrido durante o processo de atualização, o número de atualizações sem êxito, o identificador do componente do aplicativo que executa as atualizações.

- Informações sobre o uso da Kaspersky Security Network (KSN): identificador da KSN, identificador do aplicativo, versão completa do aplicativo, endereço IP despersonalizado do dispositivo do usuário, indicadores da qualidade do cumprimento das solicitações da KSN, indicadores da qualidade do processamento de pacotes da KSN, indicadores do número de solicitações da KSN e informações sobre os tipos de solicitações da KSN, data e hora do início do envio das estatísticas, data e hora do término do envio das estatísticas, informações sobre as atualizações de configuração da KSN: identificador da configuração ativa, identificador da configuração recebida, código de erro da atualização da configuração.

- Informações sobre eventos de log do sistema: hora do evento, nome do registro onde o evento foi detectado, tipo e categoria do evento, nome da fonte do evento e descrição do evento.

- Informações para determinar a reputação de arquivos e endereços URL: o endereço de URL no qual a reputação está sendo solicitada e o Referenciador, o tipo de protocolo da conexão, o identificador interno do tipo de aplicativo, o número da porta que está sendo utilizada, o identificador de Usuário, a soma de verificação do arquivo verificado (MD5), tipo de ameaça detectada, informações sobre o registro usado para detectar uma ameaça (identificador de registro para os bancos de dados de antivírus, o registro de data e hora e o tipo); chave pública do certificado; impressão digital do certificado digital do objeto verificado e algoritmo de hash.

- Dados sobre a distribuição territorial do aplicativo: data de instalação e ativação do aplicativo, ID do parceiro que fornece a licença para a ativação do aplicativo, ID do aplicativo, ID de localização do idioma do aplicativo, número de série da licença para a ativação do aplicativo, sinal de participação da KSN.

- Informações sobre a licença usada: o tipo e o período de validade da licença, número de dias até a expiração da licença, identificador do parceiro de quem a licença foi adquirida, identificador do Centro de Ativação Regional, soma de verificação do código de ativação, hash do corpo do tíquete calculado usando o algoritmo SHA1, data e hora da criação do tíquete de licença, identificador de informações da licença, identificador do tíquete de licença, identificador da sequência do tíquete de licença, identificador exclusivo do computador do usuário, data a partir da qual o tíquete de licença começa a valer, data de expiração da validade do tíquete de licença, estado atual do tíquete de licença, versão do cabeçalho do tíquete, versão da licença, identificador do certificado de assinatura do cabeçalho do tíquete, soma de verificação do arquivo de chave, número de série do assinante do cabeçalho do tíquete, token de autenticação.

- Informações sobre o hardware instalado no computador: tipo, nome, nome do modelo, versão do firmware, parâmetros de dispositivos integrados e conectados.

- Informações sobre o dispositivo: ID do dispositivo.

- Informações sobre a operação do componente Controle da Web: versão do componente, motivo da categorização, informações adicionais sobre o motivo da categorização, URL categorizado, endereço IP do host do objeto bloqueado/categorizado.

Se a infraestrutura da KSN Privada for usada pelo Kaspersky Security Center e você optar por participar da Kaspersky Security Network nas configurações da política, o Kaspersky Endpoint Security não enviará para a Kaspersky as estatísticas dos computadores clientes aos quais a política é aplicada.

Depois que a política for excluída ou desativada, as configurações da KSN em um computador cliente retornarão ao estado inicial.

Etapa 9. Defina as configurações de interação do usuário

Na janela **Interação do usuário**, defina as configurações do Kaspersky Endpoint Security para interação com o usuário do computador cliente, se necessário.

Etapa 10. Defina as configurações de conexão de rede

Na janela **Rede**, faça o seguinte, se necessário:

- Configure a conexão com um servidor proxy.
- Ative ou desative a verificação do tráfego HTTPS de entrada e saída.
- Selecione o armazenamento de certificado para verificar o tráfego HTTPS criptografado no navegador Mozilla Firefox.
- Gerencie a lista de certificados raiz confiáveis.
- Configure as portas monitoradas.

  É possível criar uma lista de portas que são monitoradas pelo Kaspersky Endpoint Security.

Etapa 11. Definir as configurações de Relatórios e Backup

Na janela **Relatórios e Backup**, faça o seguinte, se necessário:

- Defina as configurações para gerar e armazenar relatórios.
- Defina as configurações para armazenar objetos no Backup.

Etapa 12. Configure a criptografia de disco do FileVault

Na janela **Criptografia de disco FileVault**, faça o seguinte, se necessário:

- Ative ou desative o gerenciamento de criptografia de disco do FileVault para o disco de inicialização do usuário.

  Por padrão, o gerenciamento de criptografia de disco do FileVault está desativado.
- Escolha a opção **Criptografar disco**, caso deseje criptografar o disco de inicialização do usuário quando a política for aplicada a um computador cliente.

Se a caixa de seleção **Ativar o gerenciamento de criptografia de disco FileVault** estiver desmarcada, os usuários com direitos de administrador podem criptografar e descriptografar os discos de inicialização do Mac no Ajuste do Sistema.

Se a caixa de seleção **Ativar o gerenciamento de criptografia de disco FileVault** e a opção **Criptografar disco** estiverem selecionadas, os usuários com direitos de administrador não poderão descriptografar o disco de inicialização do Mac no Ajuste do Sistema.

Se a caixa de seleção **Ativar o gerenciamento de criptografia de disco FileVault** e a opção **Descriptografar disco** estiverem selecionadas, os usuários com direitos de administrador não poderão criptografar o disco de inicialização do Mac no Ajuste do Sistema.

Etapa 13. Ative o Controle da Web

Na janela **Controle da Web**, faça o seguinte, se necessário:

- Ative/desative o Controle da Web.

Nota: caso o Controle da Web para bloquear o acesso a recursos perigosos da Web seja ativado, o Kaspersky Endpoint Security exibirá a notificação **O Controle da Web está ativado** no Centro de Proteção do computador remoto.
Caso a caixa de seleção **Verificar conexões seguras (HTTPS)** esteja marcada na janela **Rede** do Assistente para Novas Políticas, o Kaspersky Endpoint Security exibirá notificações quando o usuário acessar os recursos da Web bloqueados pelo Controle da Web no computador remoto.

- Adicione uma nova regra para o Controle da Web clicando em **Adicionar**.

  Você pode inserir um nome de regra, escolher se a regra está ativa, especificar uma área de regra criando uma lista de endereços da Web específicos ou selecionando categorias de sites e uma ação que o Kaspersky Endpoint Security deve executar quando um usuário acessa um site incluído nesta regra.

- Edite, exclua ou organize as regras criadas na lista.

  A ordem em que as regras são classificadas determina a prioridade de sua aplicação pelo Kaspersky Endpoint Security.

Etapa 14. Configurar o Managed Detection and Response

Na janela **Managed Detection and Response**, caso seja necessário, faça o seguinte:

- Ative ou desative o componente Managed Detection and Response.

  Por padrão, o Managed Detection and Response está desabilitado.

- Importe ou exclua um arquivo de configuração que é usado para ativar o componente Managed Detection and Response nos dispositivos gerenciados.

Caso a caixa de seleção **Ativar Managed Detection and Response** esteja marcada e o arquivo de configuração do MDR tenha sido importado, o componente Managed Detection and Response estará ativo e interagirá com o serviço Kaspersky Managed Detection and Response. Esse serviço detecta e elimina constantemente ameaças à segurança da sua organização.

Etapa 15. Configure o Endpoint Detection and Response Expert (on-premise)

Na janela **Endpoint Detection and Response Expert (on-premise)**, caso seja necessário, faça o seguinte:

- Ative ou desative o componente Endpoint Detection and Response Expert (on-premise).

  Por padrão, o componente Endpoint Detection and Response Expert (on-premise) está desativado.

- Defina as configurações de conexão do servidor e adicione um certificado TLS.

- Adicionar um servidor.

Caso a caixa **Ativar o Endpoint Detection and Response Expert (versão 7.1 ou anterior)** esteja marcada, um certificado TLS e um servidor tenham sido adicionados, o componente Endpoint Detection and Response Expert (on-premise) ficará ativo e interagirá com a solução Kaspersky Anti Targeted Attack Platform. Essa solução detecta prontamente as ameaças avançadas, como ataques direcionados, ameaças persistentes avançadas, ataques de dia zero e outras.

Etapa 16. Configurar a verificação dos discos externos

Na janela **Verificação dos discos externos**, defina os seguintes ajustes:

- A ação que o Kaspersky Endpoint Security executa quando um disco externo é conectado.

- A ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto malicioso.

Etapa 17. Configuração da Detecção de Comportamento

Se necessário, na janela **Detecção de Comportamento**, faça o seguinte:

- Ative ou desative a Detecção de Comportamento.
  Por padrão, a Detecção de Comportamento está ativada.
- Selecione a ação a ser executada quando a atividade de malware for detectada.
- Ative ou desative a proteção de pastas compartilhadas contra criptografia externa.
  - Selecione a ação a ser executada quando a atividade de malware for detectada.

Etapa 18. Configurar Proteção Contra Ameaças ao Correio

Na janela **Proteção Contra Ameaças ao Correio**, faça o seguinte, se necessário:

- Ative ou desative a Proteção Contra Ameaças ao Correio.
  Por padrão, a Proteção Contra Ameaças à Rede está ativada.
- Selecione a ação a ser executada ao detectar um objeto malicioso.
- Configurar Proteção Contra Ameaças ao Correio.

Etapa 19. Configurar a Prevenção de Exploits

Na janela **Prevenção de Exploits**, faça o seguinte, se necessário:

- Ative ou desative a Prevenção de Exploits.
  Por padrão, a Prevenção de Exploits está ativada.
- Selecione a ação a ser executada ao detectar um exploit.

Etapa 20. Configurar o Mecanismo de Remediação

Na janela **Mecanismo de Remediação**, faça o seguinte, se necessário:

- Ative ou desative o Mecanismo de Remediação.
  Por padrão, o Mecanismo de Remediação está ativado.

Etapa 21. Ative o Controle de Dispositivos

Na janela **Controle de Dispositivos**, faça o seguinte, se necessário:

- Ative ou desative o Controle de Dispositivos.
  Por padrão, o Controle de Dispositivos está ativado.
- Defina as configurações de Controle de Dispositivos.

Etapa 22. Configurar Firewall

Na janela **Firewall**, faça o seguinte, se necessário:

- Ative ou desative o Firewall.

  Por padrão, o Firewall está ativado.

- Definir configurações de Firewall.

Etapa 23. Defina o grupo de administração ao qual a política será aplicada

Na janela **Grupo alvo**, clique em **Procurar** para selecionar um grupo de administração ao qual você deseja aplicar a política.

Etapa 24. Selecione o status da política e conclua a criação de uma política

Na janela **Criar uma política de grupo para o aplicativo**, faça o seguinte:

1. Selecione o status que será atribuído à política:

   - *Política ativa*: a política é aplicada ao grupo de administração selecionado.
   - *Política inativa:* a política não é aplicada.
   - *Política de ausência:* a política é aplicada ao grupo de administração selecionado quando os computadores estiverem desconectados da rede corporativa.

   > **Nota:** você pode criar várias políticas para um aplicativo em um grupo de administração, mas apenas uma delas pode estar ativa.

   Para obter informações detalhadas sobre status de políticas, consulte a ajuda do Kaspersky Security Center.

2. Marque a caixa de seleção **Abrir as propriedades da política imediatamente após sua criação** se desejar revisar as configurações da política após a sua criação.

3. Clique em **Finalizar** para fechar o Assistente para Novas Políticas.

   A política que você criou aparece na guia **Políticas** na área de trabalho do grupo de administração relevante. A política é aplicada aos computadores clientes após a primeira sincronização com o Servidor de Administração.

Você pode editar as configurações da política criada. Você também pode proibir ou permitir alterações em cada grupo de configurações a partir de um computador cliente usando os botões e para cada grupo de configurações. O botão ao lado de um grupo de configurações significa que o usuário de um computador cliente não tem permissão para editar essas configurações no computador do usuário. O botão ao lado de um grupo de configurações significa que o usuário de um computador cliente pode editar essas configurações no computador do usuário.

Exibir a lista de políticas

Você pode criar um número ilimitado de políticas para aplicativos instalados em computadores em cada grupo de administração, mas apenas uma política pode ser aplicada a cada aplicativo por vez em um grupo de administração.

Exibir a lista de políticas de um grupo de administração

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Selecione o grupo de administração que contém o computador cliente necessário.
5. Na área de trabalho, selecione a guia **Políticas**.

   A lista de políticas é exibida.

Definir configurações de políticas

Você pode fazer alterações em políticas criadas por você no Kaspersky Security Center e bloquear quaisquer alterações de configurações nas políticas de subgrupos e nas configurações de tarefas.

As configurações de políticas do Kaspersky Endpoint Security incluem configurações do aplicativo e configurações de tarefas.

Definir configurações de políticas

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Na área de trabalho, selecione a guia **Políticas**.
5. Clique com o botão direito na política que você deseja configurar e escolha **Propriedades**.
6. Na janela **Propriedades: <Nome da política>**, defina as configurações da política:

   - Na seção **Proteção Essencial Contra Ameaças**

     Defina as seguintes configurações de Proteção Contra Ameaças ao Arquivo

     - Ative/desative a Proteção Contra Ameaças ao Arquivo.
     - Selecione um dos níveis de segurança predefinidos ou defina as configurações de segurança manualmente.
     - Selecione a ação a ser executada ao detectar um objeto malicioso.

     Defina as seguintes configurações de Proteção Contra Ameaças da Web

     - Ative/desative a Proteção Contra Ameaças da Web.
     - Selecione um dos níveis de segurança predefinidos ou defina as configurações de segurança manualmente.

- Ative ou desative a verificação de endereços da Web no banco de dados de endereços da Web maliciosos.
- Defina as configurações de Antiphishing.
- Adicione endereços confiáveis cujo tráfego não será verificado pela Proteção Contra Ameaças da Web.
- Selecione a ação a ser executada ao detectar um objeto malicioso no tráfego da Web.

Defina as seguintes configurações de Proteção Contra Ameaças ao Correio

- Ative ou desative a Proteção Contra Ameaças ao Correio.
- Selecione a ação a ser executada ao detectar um objeto malicioso.
- Configurar Proteção Contra Ameaças ao Correio.

Defina as seguintes configurações da Proteção Contra Ameaças à Rede

- Ative/desative a Proteção Contra Ameaças à Rede.
- Defina as configurações da Proteção Contra Ameaças à Rede.
- Especifique os endereços IP dos computadores cuja atividade de rede não será bloqueada.

Defina as seguintes configurações de Firewall

- Ative ou desative o Firewall.
- Definir configurações de Firewall.

- Na seção **Proteção Avançada Contra Ameaças**
  Defina as seguintes configurações da KSN
  - Leia o texto completo da Declaração da Kaspersky Security Network, clicando em **Declaração da KSN**.
  - Ative ou desative o uso da Kaspersky Security Network.
  - Ative ou desative o modo KSN estendido.
  - Ative/desative o modo de nuvem.
  - Ative ou desative o uso de um proxy da KSN.
  - Ative ou desative o uso dos servidores da Kaspersky quando o proxy da KSN estiver indisponível.

Nota: o uso da Kaspersky Security Network e de um proxy da KSN em computadores remotos estará disponível apenas se o Servidor de Administração do Kaspersky Security Center for usado como servidor proxy. Para obter informações detalhadas sobre as propriedades do Servidor de Administração, consulte a ajuda do Kaspersky Security Center.

Defina os seguintes ajustes de Detecção de Comportamento

- Ative ou desative a Detecção de Comportamento.

  Por padrão, a Detecção de Comportamento está ativada.

- Selecione a ação a ser executada quando a atividade de malware for detectada.

Defina as seguintes configurações de Prevenção de Exploits

- Ative ou desative a Prevenção de Exploits.
- Selecione a ação a ser executada ao detectar um exploit.

Defina as seguintes configurações do Mecanismo de Remediação

Ative ou desative o Mecanismo de Remediação.

- Na seção **Controles de Segurança**

  Defina as seguintes configurações do Controle de Dispositivos

  - Ative ou desative o Controle de Dispositivos.
  - Defina as configurações de Controle de Dispositivos.

  Defina as seguintes configurações do Controle da Web

  - Ative/desative o Controle da Web.
  - Adicione uma nova regra para o Controle da Web clicando em **Adicionar**.
  - Edite, exclua ou organize as regras criadas na lista.

- Na seção **Criptografia de dados**

  Defina as seguintes configurações de criptografia de disco do FileVault

  - Ative ou desative o gerenciamento de criptografia de disco do FileVault para computadores clientes.
  - Criptografe ou descriptografe o disco de inicialização nos computadores clientes.

    Se a caixa de seleção **Ativar o gerenciamento de criptografia de disco FileVault** estiver desmarcada, os usuários com direitos de administrador podem criptografar e descriptografar os discos de inicialização do Mac no Ajuste do Sistema.

    Se a caixa de seleção **Ativar o gerenciamento de criptografia de disco FileVault** e a opção **Criptografar disco** estiverem selecionadas, os usuários com direitos de administrador não poderão descriptografar o disco de inicialização do Mac no Ajuste do Sistema.

    Se a caixa de seleção **Ativar o gerenciamento de criptografia de disco FileVault** e a opção **Descriptografar disco** estiverem selecionadas, os usuários com direitos de administrador não poderão criptografar o disco de inicialização do Mac no Ajuste do Sistema.

- Na seção **Detection and Response**

  Defina as seguintes configurações do Managed Detection and Response

  - Ative ou desative o componente Managed Detection and Response.
  - Importe ou exclua um arquivo de configuração que é usado para ativar o componente Managed Detection and Response nos dispositivos gerenciados.

Defina as seguintes configurações do Endpoint Detection and Response (KATA)

- Ative ou desative o componente Endpoint Detection and Response (KATA).
- Defina as configurações de conexão do servidor e adicione um certificado TLS.
- Adicione um servidor KATA.

- Na seção **Tarefas locais**

  Defina os seguintes ajustes da Verificação de Discos Externos

  - A ação que o Kaspersky Endpoint Security executa quando um disco externo é conectado.
  - A ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto malicioso.

- Na seção **Atualização**

  Defina as seguintes configurações de atualização

  - Ative ou desative a atualização dos módulos do aplicativo.
  - Especifique fontes de atualização.

- Na seção **Configurações adicionais**

  Defina as seguintes configurações de proteção

  - Ative ou desative a proteção em tempo real do computador cliente.
  - Ative ou desative a inicialização do Kaspersky Endpoint Security quando o computador cliente for iniciado.
  - Configure a zona confiável.
  - Configure os aplicativos confiáveis.
  - Selecione os tipos de objetos a serem detectados.
  - Desative ou ative a inicialização de tarefas agendadas quando o computador estiver funcionando com bateria.

  Defina as seguintes configurações de rede

  - Ative ou desative o uso de um servidor proxy.
  - Especifique o endereço do servidor proxy.
  - Ative ou desative o uso de um servidor proxy para endereços locais.
  - Especifique o nome de usuário e a senha para autenticação do servidor proxy.
  - Ative ou desative a verificação do tráfego HTTPS de entrada e saída.

- Selecione o armazenamento de certificado para verificar o tráfego HTTPS criptografado no navegador Mozilla Firefox.
- Configure as portas monitoradas.

Defina as configurações de Relatórios e Backup

- Ative ou desative o salvamento de eventos não críticos no relatório.
- Ative ou desative o salvamento apenas de eventos recentes.
- Ative ou desative a remoção de eventos após o período especificado.
- Especifique o período de armazenamento de eventos.
- Ative ou desative a remoção de objetos do Backup após o período especificado.
- Especifique o período de armazenamento de objetos no Backup.

Defina as seguintes configurações de interação do usuário

- Ative ou desative as notificações de eventos.
- Selecione como o Kaspersky Endpoint Security notificará o usuário sobre eventos.
- Ative ou desative a exibição do ícone do Kaspersky Endpoint Security na barra de menus.
- Defina se o usuário pode abrir a janela principal do Kaspersky Endpoint Security e usar a interface do aplicativo no computador cliente.
- Ative ou desative a disponibilidade do item **Sair** no menu de atalho do ícone do Kaspersky Endpoint Security no computador cliente.
- Selecione o idioma usado para exibir os eventos do Kaspersky Security Center.
- Defina as configurações do Kaspersky Endpoint Security disponíveis aos usuários do computador cliente.
- Configure a Proteção por senha para limitar ações indesejadas nos dispositivos do usuário.

7. Clique em **OK** para salvar as alterações e fechar a janela de propriedades da política.

Alterar o status da política

Um status de política define a operação de uma política. A política pode ter status ativo, ausente ou inativo. Você pode alterar o status da política nas configurações de política.

Alterar o status da política

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.

4. Selecione o grupo de administração que contém o computador cliente necessário.
5. Na área de trabalho, selecione a guia **Políticas**.
6. Clique com o botão direito na política cujo estado você deseja alterar e escolha **Propriedades** no menu de contexto.
7. Na janela **Propriedades:** <Nome da política>, selecione a seção **Geral**.
8. Na seção **Status da política**, selecione um dos seguintes status de política:
   - **Política ativa**. A política sempre é aplicada ao grupo de administração selecionado.
   - **Política de ausência**. A política é aplicada ao grupo de administração selecionado quando os computadores clientes estiverem desconectados da rede corporativa.
   - **Política inativa**. A política não é aplicada ao grupo de administração selecionado.
9. Clique em **OK** para salvar as alterações e fechar a janela **Propriedades: <Nome da política>**.

Exportar uma política para um arquivo KLP

Você pode exportar uma política personalizada para um arquivo para usá-la em outro Servidor de Administração.

Exportar uma política para um arquivo KLP

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Selecione o grupo de administração que contém o computador cliente necessário.
5. Na área de trabalho, selecione a guia **Políticas**.
6. Clique com o botão direito do mouse na política para exibir seu menu de contexto e escolha **Exportar**.
   A janela **Salvar como** é aberta.
7. Selecione a pasta na qual deseja salvar o arquivo KLP para a política.
8. Especifique o nome do arquivo.
9. Clique em **Salvar** para salvar o arquivo na pasta selecionada.

Importar uma política de um arquivo KLP

Você pode importar uma política existente com configurações predefinidas de um arquivo.

Importar uma política de um arquivo KLP

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, clique em **Dispositivos gerenciados**.
4. Selecione o grupo de administração que contém o computador cliente necessário.
5. Na área de trabalho, selecione a guia **Políticas**.
6. Abra a janela de seleção de arquivo de uma das seguintes maneiras:
   - Clique no botão **Importar política de arquivo**.
   - Clique com o botão direito do mouse em um espaço vazio na área de trabalho para abrir o menu de contexto e selecione o item **Importar**.
7. Selecione um arquivo KLP com uma política e clique em **Abrir**.

A política importada é adicionada à lista de políticas na área de trabalho.

Criar e gerenciar perfis da política

Um perfil da política é um conjunto nomeado de configurações variáveis para uma política, ativado em um computador cliente quando condições específicas são atendidas. A ativação de um perfil modifica as configurações da política em vigor no dispositivo quando o perfil da política é ativado.

Criar um perfil da política

1. Na árvore do console, selecione o grupo de administração para o qual deseja criar um perfil da política.
2. Na área de trabalho, selecione a guia **Políticas**.
3. Siga um destes procedimentos para abrir as propriedades da política para a qual deseja criar um perfil:
   - Clique duas vezes no nome da política.
   - Clique com o botão direito do mouse no nome da política para exibir o menu de contexto e escolha **Propriedades**.
   - Clique no link **Configurar política**.
4. Na janela **Propriedades:** <Nome da política>, selecione a seção **Perfis da política**.
5. Na área de trabalho, clique em **Adicionar**.
6. Na janela **Atribuindo perfis de política**, leia as informações sobre políticas e clique em **Avançar**.

   Se não deseja exibir esta janela ao criar novos perfis da política, marque a caixa de seleção **Não mostrar esta janela novamente** antes de clicar em **Avançar**.

7. Na janela **Nome do perfil da política**, faça o seguinte para configurar o perfil da política:

   - Insira o nome do novo perfil da política.

     Nota: o nome de um perfil não pode incluir mais de 100 caracteres.

   - Na seção **Estado no perfil da política**, selecione se o perfil da política está ativado ou desativado.
   - Na lista suspensa na seção **Estado no perfil da política**, selecione se o perfil da política pode ser editado.
   - Caso queira configurar regras de ativação para o perfil da política, marque a caixa de seleção **Após fechar o assistente de novo perfil da política, siga para a configuração da regra de ativação do perfil da política**.

8. Clique em **Finalizar**.

9. Caso a caixa de seleção **Após fechar o assistente de novo perfil da política, siga para a configuração da regra de ativação do perfil da política** seja marcada, siga as etapas do assistente para regras de ativação de novos perfis da política.

O perfil de política criado por você é exibido na seção **Perfis da política** da janela **Propriedades:** <Nome da política>.

Criar uma regra de ativação do perfil da política

1. Na árvore do console, selecione o grupo de administração no qual deseja criar uma regra de ativação do perfil da política.

2. Na área de trabalho, selecione a guia **Políticas**.

3. Siga um destes procedimentos para abrir as propriedades da política:

   - Clique duas vezes no nome da política.
   - Clique com o botão direito do mouse no nome da política para exibir o menu de contexto e escolha **Propriedades**.
   - Clique no link **Configurar política**.

4. Na janela **Propriedades: <Nome da política>**, selecione a seção **Perfis da política**.

5. Na área de trabalho, selecione o perfil da política para o qual deseja criar uma regra de ativação e clique em **Propriedades**.

   A janela **Propriedades: <Nome do perfil da política>** é aberta.

6. Selecione a seção **Regras de ativação**.

7. Na área de trabalho, clique em **Adicionar**.

   O assistente para regras de ativação de novos perfis da política é iniciado.

Siga as etapas do assistente para regras de ativação de novos perfis da política.

Alterar um perfil da política

1. Na árvore do console, selecione o grupo de administração para o qual deseja alterar um perfil da política.
2. Na área de trabalho, selecione a guia **Políticas**.
3. Siga um destes procedimentos para abrir as propriedades de política para as quais deseja alterar um perfil:
   - Clique duas vezes no nome da política.
   - Clique com o botão direito do mouse no nome da política para exibir o menu de contexto e escolha **Propriedades**.
   - Clique no link **Configurar política**.
4. Na janela **Propriedades: <Nome da política>**, selecione a seção **Perfis da política**.
5. Na área de trabalho, selecione o perfil da política que deseja alterar e clique em **Propriedades**.

   A janela **Propriedades: <Nome do perfil da política>** é aberta.
6. Configure o perfil, conforme necessário:
   - Na seção **Geral**, renomeie o perfil ou ative/desative o perfil, marcando/desmarcando a caixa de seleção **Ativar perfil**.
   - Na seção **Regras de ativação**, crie, edite ou exclua as regras de ativação.
   - Na seção **Dispositivos**, escolha os dispositivos aos quais o perfil da política é aplicado.
   - Edite as configurações de política nas seções relevantes.
7. Clique em **OK**.

Se o perfil da política estiver ativo, as configurações alteradas serão aplicadas após o computador cliente ser sincronizado com o Servidor de Administração. Se o perfil da política estiver inativo, elas serão aplicadas depois que a regra de ativação for acionada.

Alterar a prioridade de um perfil da política

1. Na árvore do console, selecione o grupo de administração para o qual deseja alterar a prioridade de um perfil da política.
2. Na área de trabalho, selecione a guia **Políticas**.
3. Siga um destes procedimentos para abrir as propriedades da política para a qual deseja alterar a prioridade de um perfil da política:
   - Clique duas vezes no nome da política.
   - Clique com o botão direito do mouse no nome da política para exibir o menu de contexto e escolha **Propriedades**.
   - Clique no link **Configurar política**.
4. Na janela **Propriedades: <Nome da política>**, selecione a seção **Perfis da política**.

5. Na área de trabalho, selecione o perfil da política cuja prioridade deseja alterar.

6. Aumente/diminua a prioridade do perfil selecionado clicando nos botões  .

Excluir um perfil da política

1. Na árvore do console, selecione o grupo de administração para o qual deseja excluir um perfil da política.

2. Na área de trabalho, selecione a guia **Políticas**.

3. Siga um destes procedimentos para abrir as propriedades da política para a qual deseja excluir um perfil:

   - Clique duas vezes no nome da política.
   - Clique com o botão direito do mouse no nome da política para exibir o menu de contexto e escolha **Propriedades**.
   - Clique no link **Configurar política**.

4. Na janela **Propriedades: <Nome da política>**, selecione a seção **Perfis da política**.

5. Na área de trabalho, selecione o perfil que deseja excluir e clique em **Excluir**.

Para informações detalhadas sobre perfis de política, consulte a ajuda do Kaspersky Security Center Help.

Gerar um relatório sobre objetos detectados

Gerar um relatório sobre objetos detectados

1. Inicie o Console de Administração do Kaspersky Security Center.

2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.

3. Na árvore do console, clique em **Dispositivos gerenciados**.

4. Selecione o grupo de administração que contém o computador cliente necessário.

5. Selecione a guia **Dispositivos**.

6. Selecione o computador na lista de computadores clientes.

7. Clique com o botão direito do mouse no computador selecionado para abrir o menu de contexto e escolha **Todas as tarefas** > **Exibir o relatório sobre ameaças**.

O relatório gerado será aberto em uma janela do navegador.

É possível encontrar informações em relação a outras maneiras de gerar um relatório sobre os objetos detectados pelo aplicativo no computador cliente na ajuda do Kaspersky Security Center.

Obter uma chave de recuperação para uma unidade criptografada

Se um usuário de um computador cliente esquecer ou perder as suas credenciais e não puder acessar um disco criptografado, será possível obter uma chave de recuperação.

Obter uma chave de recuperação

1. Inicie o Console de Administração do Kaspersky Security Center.
2. Maximize o nó do **Servidor de Administração <Nome do servidor>**.
3. Na árvore do console, selecione a pasta **Avançado**, a subpasta **Criptografia e proteção de dados** e, em seguida, a subpasta **Unidades criptografadas**.
4. Na área de trabalho, clique com o botão direito do mouse no dispositivo com o disco criptografado para exibir o menu de atalho e selecione **Obter chave de recuperação para macOS**.

   Uma janela com a chave de recuperação é aberta.
5. Salve a chave de recuperação do modo que considerar conveniente.

É possível usar essa chave de recuperação em um computador cliente para acessar a unidade criptografada.

Administração remota do aplicativo por meio do Web Console e do Kaspersky Security Center Cloud Console

O Kaspersky Security Center Web Console (Web Console) é um aplicativo da Web destinado a fornecer uma maneira centralizada de executar as principais tarefas de gerenciamento e manutenção da segurança da rede de uma organização. O Web Console é um componente do Kaspersky Security Center que fornece uma interface de usuário para o gerenciamento do Kaspersky Endpoint Security em uma janela de navegador. Para obter informações detalhadas sobre o Kaspersky Security Center Web Console, consulte a Ajuda do Kaspersky Security Center.

O Kaspersky Security Center Cloud Console (Cloud Console) é uma solução baseada na nuvem para proteger e gerenciar a rede de uma organização. Para obter informações detalhadas sobre o Kaspersky Security Center Cloud Console, consulte a Ajuda do Kaspersky Security Center Cloud Console.

Também é possível gerenciar o Kaspersky Endpoint Security na interface gráfica do usuário do aplicativo, no Console de Administração do Kaspersky Security Center e usando a linha de comando.

Instalar o plug-in da web do Kaspersky Endpoint Security

O plug-in da web do Kaspersky Endpoint Security permite a interação entre o Kaspersky Endpoint Security e o Kaspersky Security Center. O plug-in da web deve ser instalado em um dispositivo que tenha o Kaspersky Security Center Web Console instalado. A funcionalidade do plug-in da web está disponível para todos os administradores que têm acesso ao Kaspersky Security Center Web Console em um navegador.

Você pode instalar o plug-in da web da seguinte forma:

- Usando o Assistente de Início Rápido do Kaspersky Security Center Web Console.

  O Web Console solicita automaticamente que você execute o Assistente de Início Rápido ao conectar o Web Console ao Servidor de Administração pela primeira vez. Também é possível executar o Assistente de início rápido na interface do Web Console (**Descoberta e implementação** → **Implementação e atribuição** → **Assistente de início rápido**). O Assistente de Início Rápido também pode verificar se os plug-ins da Web instalados estão atualizados e baixar as atualizações necessárias. Para obter mais detalhes sobre o Assistente de Início Rápido do Kaspersky Security Center Web Console, consulte a Ajuda do Kaspersky Security Center.

- Manualmente, usando um pacote de distribuição para o Web Console a partir de uma fonte externa.

  Para instalar o plug-in da Web, adicione o arquivo comprimido ZIP do pacote de distribuição no plug-in da Web do Kaspersky Endpoint Security na interface do Web Console: (**Configurações** → **Plug-ins da web**). O pacote de distribuição do plug-in da web pode ser baixado no site da Kaspersky.

Para instalar o plug-in da web do Kaspersky Endpoint Security manualmente:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Configurações** → **Plug-ins da web**.

   Uma lista de plug-ins da web instalados é aberta.

2. Inicie a instalação do plug-in da web do Kaspersky Endpoint Security de uma das seguintes formas:

- Instalação usando a lista de plug-ins da web da Kaspersky:

  a. Clique em **Adicionar**.

  Uma lista de todos os plug-ins da web da Kaspersky disponíveis é aberta. A lista é atualizada automaticamente depois que novas versões de plug-ins da web são lançadas.

  b. Encontre o plug-in da web do Kaspersky Endpoint Security for Mac 12.2.1 na lista e clique nele.

  c. Na janela com uma descrição do plug-in da Web, clique no botão **Instalar o plug-in**.

  d. Aguarde a conclusão da instalação e clique em **OK** na janela de informações.

- Instalação do plug-in da web usando uma fonte externa (os arquivos necessários para instalar os plug-ins da web estão incluídos no kit de distribuição):

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

  b. Na janela que é aberta, especifique o caminho para o arquivo ZIP com o kit de distribuição para o plug-in da web e o caminho para o arquivo de assinatura no formato TXT. Este arquivo faz parte do arquivo compactado com o plug-in da web.

  c. Clique em **Adicionar**.

  d. Aguarde a conclusão da instalação e clique em **OK** na janela de informações.

O novo plug-in é exibido na lista de plug-ins da Web instalados (**Configurações** → **Plug-ins da web**).

Nota: se você selecionar um idioma que não esteja incluído no pacote de distribuição do Kaspersky Endpoint Security nas propriedades do Servidor de Administração do Kaspersky Security Center, o Contrato de Licença e toda a interface do Kaspersky Security Center Web Console serão exibidos em inglês.

Criar uma política

Esta seção contém informações sobre como criar e configurar políticas para o Kaspersky Endpoint Security usando o Web Console e o Kaspersky Security Center Cloud Console.

Uma política determina as configurações de um aplicativo e gerencia a capacidade de configurar esse aplicativo em dispositivos dentro de um grupo de administração. Uma política individual deve ser criada para cada aplicativo. É possível criar um número ilimitado de políticas para aplicativos instalados em dispositivos em cada grupo de administração, mas apenas uma política pode ser aplicada a cada aplicativo por vez em um grupo de administração.

Nota: ao criar e configurar uma política, você pode permitir ou proibir alterações a qualquer grupo de configurações nas políticas usando o botão **Aplicar**.

Criar uma política

1. Na seção **Dispositivos**, à esquerda, selecione a seção **Políticas e perfis**.
2. Clique em **Adicionar**.
3. Selecione o aplicativo para o qual deseja criar uma política e clique em **Avançar**.

   A janela **Nova política** é aberta.
4. Na guia **Geral**, especifique o nome da política e configure o status da política, além das opções de herança das configurações da política.
5. Na guia **Configurações do aplicativo**, defina as configurações do aplicativo que serão aplicadas ao Kaspersky Endpoint Security no computador cliente quando a política for aplicada.
6. Clique em **Salvar**.

Você pode executar as seguintes ações em políticas personalizadas:

- Criar políticas.
- Configurar políticas.
- Copiar ou mover políticas de um grupo para outro.
- Excluir políticas.
- Alterar o status de políticas.

Para obter informações detalhadas sobre as políticas do Kaspersky Security Center Web Console, consulte a ajuda do Kaspersky Security Center.

Para obter informações detalhadas sobre as políticas do Kaspersky Security Center Cloud Console, consulte a ajuda do Kaspersky Security Center Cloud Console.

Nota: depois de criar um perfil da política para uma política do Kaspersky Endpoint Security usando o Kaspersky Security Center Web Console e o Cloud Console, é necessário verificar se as configurações foram aplicadas corretamente nos computadores clientes.

Proteção contra ameaças ao host

Configure o componente Proteção Contra Ameaças ao Arquivo

É possível configurar o componente Proteção Contra Ameaças ao Arquivo de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Proteção Contra Ameaças ao Host → Proteção Contra Ameaças ao Arquivo**.
  5. Ative ou desative o componente usando o botão de alternância **Proteção Contra Ameaças ao Arquivo**.
  6. Configure o componente Proteção Contra Ameaças ao Arquivo.
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Proteção Essencial Contra Ameaças → Proteção Contra Ameaças ao Arquivo**.
  5. Ative ou desative o componente usando o botão de alternância **Proteção Contra Ameaças ao Arquivo**.
  6. Configure o componente Proteção Contra Ameaças ao Arquivo.
  7. Salve suas alterações.

Configurações de Proteção Contra Ameaças ao Arquivo

Configurações	Descrição
Exclusões de verificação	Uma *exclusão de verificação* é um conjunto de condições que devem ser atendidas para que o Kaspersky Endpoint Security não verifique um determinado objeto em busca de vírus e 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 explorados por invasores. Para obter detalhes sobre os aplicativos legítimos que os intrusos podem usar para danificar o computador ou os dados pessoais, visite o site da Kaspersky IT Encyclopedia.
Ação ao detectar ameaça	**Desinfectar e excluir se a desinfecção falhar** Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo. **Perguntar o que fazer**. O Kaspersky Endpoint Security exibe uma janela de notificações com informações sobre o objeto malicioso que infectou o arquivo e solicita que você escolha a ação a ser executada pelo Kaspersky Endpoint Security. As ações disponíveis podem variar dependendo do status do objeto.

Configurações	Descrição
Escopo de proteção	Contém objetos que são verificados pelo componente Proteção Contra Ameaças ao Arquivo. Um objeto de verificação pode ser um disco rígido, unidade removível, unidade de rede, pasta, arquivo ou arquivos múltiplos, definido por uma máscara. Por padrão, o componente Proteção Contra Ameaças ao Arquivo verifica somente arquivos iniciados em discos rígidos, unidades de rede ou unidades removíveis. O escopo de proteção para esses objetos não pode ser alterado ou excluído. Você também pode excluir um objeto (como unidades removíveis) das verificações.
Otimização da verificação	Abaixo de **Otimização da verificação**, você pode configurar o Kaspersky Endpoint Security para obter melhor desempenho ao verificar arquivos. • **Verificar apenas arquivos novos e modificados**. Verifica apenas os arquivos novos e aqueles que foram modificados desde a última vez em que foram verificados. Isso ajuda a reduzir a duração de uma verificação. Esse modo se aplica a arquivos simples e compostos. • **Ignorar a verificação de volumes de sistema somente leitura**. Se esta caixa de seleção estiver marcada, o aplicativo não verificará o volume do sistema somente leitura. Isso reduz significativamente o tempo de verificação.
Verificação de 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. • **Verificar arquivos compactados**. Verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos compactados. O aplicativo verifica os arquivos por extensão e formato. Ao verificar os arquivos, o aplicativo executa uma descompactação recursiva. Isso permite detectar ameaças em arquivos multinível (arquivo dentro de arquivo). • **Verificar pacotes de distribuição e arquivos compactados autoextraíveis**. Verificação de pacotes de instalação de aplicativos de terceiros e arquivos comprimidos de extração automática. Os arquivos comprimidos de extração automática integram um módulo de extração executável. Para verificar arquivos comprimidos de extração automática, a caixa de seleção **Verificar arquivos compactados** deve ser selecionada. • **Verificar arquivos em formatos do Microsoft Office e objetos OLE incorporados**. Arquivos do Microsoft Office (por exemplo, DOC, DOCX, XLS, PPT) e objetos OLE incorporados em arquivos (por exemplo, tabelas do Excel, macros, anexos de e-mail).
Permitir descompactação em segundo plano de arquivos maiores que (MB)	Se essa caixa de seleção estiver selecionada, o aplicativo fornece acesso a arquivos compostos maiores que o valor especificado antes da verificação desses arquivos. Nesse caso, o Kaspersky Endpoint Security descompacta e verifica os arquivos compostos em segundo plano. O aplicativo fornece acesso a arquivos compostos menores que esse valor somente após descompactar e verificar esses arquivos. Se a caixa de seleção não estiver selecionada, o aplicativo Kaspersky Endpoint Security fornecerá acesso a arquivos compostos somente após descompactar e verificar arquivos de qualquer tamanho.
Não verificar arquivos compactados com mais de (MB)	Se esta caixa de seleção for marcada, o aplicativo não verificará arquivos compostos se o tamanho deles exceder o valor especificado. Se esta caixa de seleção estiver desmarcada, o aplicativo verificará os arquivos compostos de todos os tamanhos. O aplicativo verifica arquivos grandes extraídos de arquivos compactados independentemente de a caixa de seleção estar selecionada ou não.

Configure a Verificação de Unidades Removíveis

É possível configurar o componente Verificação de Unidades Removíveis de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Proteção Contra Ameaças ao Host → Verificação de unidades removíveis**.
  5. Ative ou desative o componente usando o botão de alternância **Verificação de Unidades Removíveis**.

6. Configure o componente Verificação de Unidades Removíveis.
7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Tarefas locais → Verificação dos discos externos**.
5. Configure o componente Verificação de Unidades Removíveis.
6. Salve suas alterações.

Configuração da Detecção de Comportamento

É possível configurar o componente Detecção de Comportamento de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para a seção **Proteção Contra Ameaças ao Host → Análise de comportamento → Detecção de Comportamento**.
5. Ative ou desative o componente usando o botão de alternância **Detecção de Comportamento**.
6. Configure o componente Detecção de Comportamento.
7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção Avançada Contra Ameaças → Detecção de Comportamento**.
5. Ative ou desative o componente usando o botão de alternância **Detecção de Comportamento**.

6. Configure o componente Detecção de Comportamento.
7. Salve suas alterações.

Configurações de Detecção de Comportamento

Configurações	Descrição
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 monitora todos os objetos que são abertos, executados ou salvos por qualquer processo do aplicativo e controla a atividade de todos os aplicativos e tráfego de rede criada por eles. Depois que um aplicativo é adicionado à lista de aplicativos confiáveis, o Kaspersky Endpoint Security para de monitorar a atividade do aplicativo.
Exclusões de verificação	Uma *exclusão de verificação* é um conjunto de condições que devem ser atendidas para que o Kaspersky Endpoint Security não verifique um determinado objeto em busca de vírus e 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 explorados por invasores. Para obter detalhes sobre os aplicativos legítimos que os intrusos podem usar para danificar o computador ou os dados pessoais, visite o site da Kaspersky IT Encyclopedia.
Ação ao detectar ameaça	**Solicitar ação**. Caso uma atividade maliciosa seja detectada, o Kaspersky Endpoint Security solicitará que o usuário selecione a ação que deverá ser executada neste momento. As ações disponíveis podem variar dependendo do status do objeto. **Bloquear**. Caso alguma atividade maliciosa seja detectada, o Kaspersky Endpoint Security bloqueará o aplicativo que está executando a atividade maliciosa e registrará em log as informações sobre a atividade detectada. **Excluir**. Caso esta opção esteja selecionada, ao detectar uma atividade maliciosa, o Kaspersky Endpoint Security excluirá o arquivo executável do aplicativo malicioso e criará uma cópia de backup do arquivo no Backup.

Configuração do Anti-Cryptor

É possível configurar o componente Anti-Cryptor de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**
  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Proteção Contra Ameaças ao Host → Análise de comportamento → Anticryptor**.
  5. Ative ou desative o componente usando o botão de alternância **Anti-Cryptor**.
  6. Configure o componente Anti-Cryptor.
  7. Salve suas alterações.
- **Uso do plug-in do Kaspersky Endpoint Security**
  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Proteção Avançada Contra Ameaças → Detecção de Comportamento**.

5. Use o botão de alternância **Proteger pastas compartilhadas contra criptografia externa** para ativar ou desativar o componente.
6. Configure o componente Anti-Cryptor.
7. Salve suas alterações.

Configurações do Anti-Cryptor

Parâmetro	Descrição
Ação ao detectar ameaça	**Informar**. Caso esta opção seja selecionada, ao detectar uma tentativa de modificação de arquivos em pastas compartilhadas, o Kaspersky Endpoint Security adiciona informações sobre esta tentativa na lista de ameaças ativas, além de adicionar uma entrada no relatório. **Bloquear conexão por (min)**. Ao detectar uma tentativa de modificação de arquivos em pastas compartilhadas, o Kaspersky Endpoint Security bloqueia o tráfego de rede de um dispositivo que executa atividades maliciosas. O aplicativo cria um evento *Criptografia detectada* que contém informações sobre o dispositivo comprometido.

Configuração do componente Prevenção de Exploits

É possível configurar o componente Prevenção de Exploits de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**
  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Proteção Contra Ameaças ao Host → Análise de comportamento → Prevenção de Exploits**.
  5. Ative ou desative o componente usando botão de alternância **Prevenção de Exploits**.
  6. Configure o componente Prevenção de Exploits.
  7. Salve suas alterações.
- **Uso do plug-in do Kaspersky Endpoint Security**
  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Proteção Avançada Contra Ameaças → Prevenção de Exploits**
  5. Ative ou desative o componente usando botão de alternância **Prevenção de Exploits**.
  6. Configure o componente Prevenção de Exploits.
  7. Salve suas alterações.

Configurações de Prevenção de exploit

Configurações	Descrição
Ação ao detectar ameaça	**Informar**. Caso este item seja selecionado, quando o Kaspersky Endpoint Security detectar um exploit, ele registrará uma entrada contendo as informações sobre o exploit e adicionará essas informações na lista de ameaças ativas. **Bloquear**. Se esse item for selecionado ao detectar uma exploit, o Kaspersky Endpoint Security bloqueará as operações dessa exploit e registrará as informações sobre ela.

Configuração do componente Mecanismo de Remediação

É possível configurar o componente Mecanismo de Remediação de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Proteção Contra Ameaças ao Host → Análise de comportamento → Mecanismo de Remediação**.
  5. Ative ou desative o componente usando o botão de alternância **Mecanismo de Remediação**.
  6. Configure o componente Mecanismo de Remediação.
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Proteção Avançada Contra Ameaças → Mecanismo de Remediação**.
  5. Ative ou desative o componente usando o botão de alternância **Mecanismo de Remediação**.
  6. Configure o componente Mecanismo de Remediação.
  7. Salve suas alterações.

Comunicação e Proteção da Web

Configurar Proteção Contra Ameaças ao Correio

É possível configurar o componente Proteção Contra Ameaças ao Correio de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Comunicação e Proteção na Web → Proteção Contra Ameaças ao Correio**.
  5. Ative ou desative o componente usando o botão de alternância **Proteção Contra Ameaças ao Correio**.
  6. Configure o componente Proteção Contra Ameaças ao Correio.
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Proteção Essencial Contra Ameaças → Proteção Contra Ameaças da Web**.
  5. Ative ou desative o componente usando o botão de alternância **Proteção Contra Ameaças ao Correio**.
  6. Configure o componente Proteção Contra Ameaças ao Correio.
  7. Salve suas alterações.

Ajustes da Proteção Contra Ameaças ao Correio

Configurações	Descrição
Ação ao detectar ameaça	**Desinfectar e excluir se a desinfecção falhar** Quando um objeto infectado é detectado em uma mensagem de entrada ou saída, o aplicativo tentará desinfectá-lo. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo excluirá o objeto infectado. O aplicativo adiciona informações sobre a ação executada ao assunto da mensagem: *[A mensagem foi processada] <assunto da mensagem>*. **Bloquear**. Caso um objeto infectado seja detectado em uma mensagem recebida, o aplicativo adiciona um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Caso um objeto infectado seja detectado em uma mensagem de saída, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro.
Não verificar arquivos compactados com mais de (MB)	Se esta caixa de seleção for marcada, o componente Proteção contra ameaças de correio excluirá arquivos compactados anexados a mensagens de e-mail da verificação se o seu tamanho exceder o valor especificado. Se a caixa de seleção for desmarcada, o componente Proteção contra ameaças de correio verificará arquivos compactados de anexo de e-mail de qualquer tamanho.
Ignorar arquivo verificado por mais de (seg)	Se a caixa de seleção for marcada, o tempo alocado para verificar arquivos compactados anexados a mensagens de e-mail será limitado ao período especificado.

Configuração do componente Proteção Contra Ameaças da Web

É possível configurar o componente Proteção Contra Ameaças à Rede de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Comunicação e Proteção na Web → Proteção Contra Ameaças da Web**.
  5. Ative ou desative o componente usando o botão de alternância **Proteção Contra Ameaças da Web**.
  6. Configure o componente Proteção Contra Ameaças da Web.
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Proteção Essencial Contra Ameaças → Proteção Contra Ameaças da Web**.
  5. Ative ou desative o componente usando o botão de alternância **Proteção Contra Ameaças da Web**.
  6. Configure o componente Proteção Contra Ameaças da Web.
  7. Salve suas alterações.

Configurações de Proteção Contra Ameaças da Web

Configurações	Descrição
Endereços da Web confiáveis	Lista de endereços da Web considerados confiáveis pela Proteção Contra Ameaças da Web. O componente não analisa o tráfego de entrada e saída desses endereços em busca de ameaças. A lista de endereços confiáveis pode ser útil, por exemplo, se o componente Proteção Contra Ameaças da Web interferir no download de um arquivo de um site conhecido.
Exclusões de verificação	Uma *exclusão de verificação* é um conjunto de condições que devem ser atendidas para que o Kaspersky Endpoint Security não verifique um determinado objeto em busca de vírus e 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 explorados por invasores. Para obter detalhes sobre os aplicativos legítimos que os intrusos podem usar para danificar o computador ou os dados pessoais, visite o site da Kaspersky IT Encyclopedia .
Ação ao detectar ameaça	**Bloquear**. Se esta opção for selecionada, quando o componente Proteção Contra Ameaças da Web detectar um objeto infectado no tráfego da Web, ele bloqueará o acesso ao objeto e exibirá uma notificação no navegador. **Solicitar ação**. O Kaspersky Endpoint Security exibe uma notificação com informações sobre o tipo de malware que infectou o objeto de tráfego da Web e solicita que você escolha a ação que o Kaspersky Internet Security deve executar nesse objeto. As ações disponíveis podem variar dependendo do status do objeto.

Configure a Proteção Contra Ameaças à Rede

É possível configurar o componente Proteção Contra Ameaças à Rede de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Comunicação e Proteção na Web → Proteção Contra Ameaças à Rede**.
  5. Ative ou desative o componente usando o botão de alternância **Proteção Contra Ameaças à Rede**.
  6. Configure o componente Proteção Contra Ameaças à Rede.
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Proteção Essencial Contra Ameaças → Proteção Contra Ameaças à Rede**.
  5. Ative ou desative o componente usando o botão de alternância **Proteção Contra Ameaças à Rede**.
  6. Configure o componente Proteção Contra Ameaças à Rede.
  7. Salve suas alterações.

Configurações de Proteção contra ameaças à rede

Configurações	Descrição
Endereços IP confiáveis	Lista de endereços IPs de dispositivos confiáveis. O componente Proteção Contra Ameaças à Rede não bloqueia a atividade de rede desses endereços.
Ação ao detectar ameaça	**Bloquear**. Quando uma ameaça é detectada, a Proteção Contra Ameaças à Rede bloqueia o ataque. **Bloquear o ataque e o dispositivo de ataque durante (min)**. Caso esta opção seja ativada, o componente Proteção Contra Ameaças à Rede adicionará o computador atacante à lista bloqueada. Isso significa que o componente Proteção Contra Ameaças à Rede bloqueia a conexão de rede com o computador de ataque depois da primeira tentativa de ataque de rede pelo período de tempo especificado. Esse bloqueio protege automaticamente o computador do usuário contra a ocorrência de ataques de rede futuros que se originem do mesmo endereço. O tempo mínimo que um computador atacante deve gastar na lista de bloqueio é um minuto. O tempo máximo é de 999 minutos.

Configure o componente Firewall

É possível configurar o componente Firewall de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Comunicação e Proteção na Web → Firewall**.
  5. Ative ou desative o componente usando o botão de alternância **Firewall**.
  6. Configure o componente Firewall.
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Proteção Essencial Contra Ameaças → Firewall**.
  5. Ative ou desative o componente usando o botão de alternância **Firewall**.
  6. Configure o componente Firewall.
  7. Salve suas alterações.

Configurações	Descrição
Regras de pacotes de rede	Tabela com uma lista de regras de pacotes de rede. As regras de pacotes de rede tem a função de impor restrições a pacotes de rede, seja qual for o aplicativo. Estas regras restringem o tráfego de rede de entrada e de saída através de portas específicas do protocolo de dados selecionado. A tabela lista regras de pacotes de rede pré-configuradas recomendadas pela Kaspersky para a proteção ideal do tráfego de rede de computadores que executam sistemas operacionais macOS. O Firewall estabelece a prioridade de execução de cada regra de pacotes de rede. O Firewall processa as regras de pacotes de rede na ordem em que aparecem na lista de regras de pacote de rede, ou seja, de cima para baixo. O Firewall localiza e aplica a regra de pacotes de rede no topo da lista que mais está adequada a conexão de rede, permitindo ou bloqueando a atividade de rede. O Firewall ignora todas as regras do pacote de rede subsequentes para a conexão de rede específica. As regras de pacotes de rede têm prioridade sobre as regras de rede dos aplicativos.
Redes disponíveis	Esta tabela contém informações sobre conexões da rede que o Firewall detecta no computador. Os seguintes tipos de conexão de rede estão disponíveis: • A rede não está protegida por aplicativos antimalware, firewalls ou filtros (como Wi-Fi em um café). Quando o usuário opera um computador conectado a essa rede, o Firewall bloqueia o acesso a arquivos e impressoras desse computador. Os usuários externos também não podem acessar dados por meio de pastas compartilhadas e acesso remoto à área de trabalho deste computador. O Firewall filtra a atividade de rede de cada aplicativo, de acordo com as regras de rede definidas para cada uma. • Rede para usuários com acesso restrito a arquivos e impressoras neste computador (como para uma LAN ou rede doméstica). • Rede segura na qual o computador não é exposto a ataques ou tentativas não autorizadas de acesso a dados. O Firewall permite qualquer atividade de rede dentro de redes com esse status.

Controles de Segurança

Configuração do componente Controle de Dispositivos

É possível configurar o componente Controle de Dispositivos de das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Controles de Segurança → Controle de dispositivos**.
  5. Ative ou desative o componente usando o botão de alternância **Controle de Dispositivos**.
  6. Ative o Controle de Dispositivos
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Controles de Segurança → Controle de Dispositivos**.
  5. Ative ou desative o componente usando o botão de alternância **Controle de Dispositivos**.
  6. Ative o Controle de Dispositivos
  7. Salve suas alterações.

Configurações do Controle de dispositivos

Configurações	Descrição
Dispositivos confiáveis	Lista de dispositivos e usuários confiáveis aos quais é concedido acesso a esses dispositivos.
Dispositivos e redes Wi-Fi	Uma lista de todos os tipos dispositivo disponíveis segundo a classificação do componente Controle de Dispositivos, inclusive os seus respectivos status de acesso.

Configuração do componente Controle da Web

É possível configurar o componente Controle da Web de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Controles de Segurança → Controle da Web**.
  5. Ative ou desative o componente usando o botão de alternância **Controle da Web**.
  6. Configure o componente Controle da Web.
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.

3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controles de Segurança → Controle da Web**.
5. Ative ou desative o componente usando o botão de alternância **Controle da Web**.
6. Configure o componente Controle da Web.
7. Salve suas alterações.

Configurações do Controle da Web

Configurações	Descrição
Lista de regras	Lista contendo regras de acesso de recurso da Web. Cada regra tem uma prioridade. Quanto mais alta uma regra estiver na lista, mais alta será sua prioridade. Se um site foi adicionado a várias regras, o Controle da Web regula o acesso ao site com base na regra com a maior prioridade.
Ação padrão	A regra de acesso aos recursos da Web que não são abrangidos por nenhuma outra regra. As seguintes opções estão disponíveis: • **Permitir tudo, exceto a lista de regras**. • **Bloquear tudo, exceto a lista de regras**.

Criptografia de Dados

É possível configurar o componente Criptografia de dados de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**
  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Criptografia de dados**.
  5. Ative ou desative o componente usando o botão de alternância **Criptografia de dados**.
  6. Configure o componente Criptografia de dados.
  7. Salve suas alterações.
- **Uso do plug-in do Kaspersky Endpoint Security**
  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Criptografia de dados**.
  5. Ative ou desative o componente usando o botão de alternância **Criptografia de disco FileVault**.

6. Configure o componente Criptografia de dados.
7. Salve suas alterações.

Configurações de criptografia completa do disco

Configurações	Descrição
Ação sobre os dispositivos	**Criptografar todos os discos rígidos**. Caso esta opção seja selecionada, o aplicativo criptografará todos os discos rígidos quando a política for aplicada. **Descriptografar todos os discos rígidos**. Caso esta opção seja selecionada o aplicativo descriptografará todos os discos rígidos anteriormente criptografados quando a política for aplicada.

Configurações gerais

Configurações de detecção

É possível definir as configurações de detecção de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**
  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Configurações gerais → Configurações de detecção**.
  5. Defina as configurações de detecção.
  6. Salve suas alterações.
- **Uso do plug-in do Kaspersky Endpoint Security**
  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Configurações adicionais → Proteção**.
  5. Defina as configurações de detecção.
  6. Salve suas alterações.

Configurações de detecção

Configurações	Descrição
Detecção de outros tipos de objetos	Independentemente das configurações definidas para o aplicativo, o Kaspersky Endpoint Security sempre detecta e bloqueia vírus, worms, cavalos de Troia e ferramentas maliciosas. Eles podem causar grandes danos ao computador. Você também pode ativar a detecção dos seguintes tipos de objetos: • **Software legítimo que pode ser usado por intrusos para danificar seu computador ou dados pessoais**. Embora não tenham nenhuma atividade maliciosa, esses aplicativos podem ser explorados por invasores. Para obter detalhes sobre os aplicativos legítimos que os intrusos podem usar para danificar o computador ou os dados pessoais, visite o site da Kaspersky IT Encyclopedia.

Kaspersky Security Network

É possível definir as configurações da Kaspersky Security Network de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Configurações gerais → Kaspersky Security Network**.
  5. Marque ou desmarque a opção **Kaspersky Security Network (KSN)** para ativar ou desativar o componente.
  6. Configure o componente da Kaspersky Security Network.
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Proteção Avançada Contra Ameaças → Kaspersky Security Network**.
  5. Marque ou desmarque a opção **Kaspersky Security Network** para ativar ou desativar o componente.
  6. Configure o componente da Kaspersky Security Network.
  7. Salve suas alterações.

Configurações de detecção

Configurações	Descrição
Usar modo KSN estendido	O *modo KSN estendido* é um modo no qual o Kaspersky Endpoint Security envia dados adicionais para a Kaspersky. O Kaspersky Endpoint Security usa o KSN para detectar ameaças independentemente da posição do botão de alternância.
Usar o modo na nuvem	O *Modo nuvem* refere-se ao modo operacional do aplicativo no qual o Kaspersky Endpoint Security usa uma versão simplificada dos bancos de dados de antivírus. A Kaspersky Security Network oferece suporte ao funcionamento do aplicativo quando bancos de dados de antivírus leves estão em uso. A versão leve dos bancos de dados de antivírus permite usar aproximadamente metade da RAM do computador que, de outra forma, seria usada nos bancos de dados comuns. Se você não participa da Kaspersky Security Network ou se o modo de nuvem está desativado, o Kaspersky Endpoint Security faz o download da versão completa dos bancos de dados antivírus dos servidores da Kaspersky. Se a caixa de seleção estiver marcada, o Kaspersky Endpoint Security usará a versão simplificada dos bancos de dados de antivírus, o que reduz a carga nos recursos do sistema operacional. O Kaspersky Endpoint Security baixará a versão leve dos bancos de dados antivírus durante a próxima atualização depois que a caixa de seleção for marcada. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security usará a versão completa dos bancos de dados de antivírus. O Kaspersky Endpoint Security baixará a versão completa dos bancos de dados antivírus durante a próxima atualização depois que a caixa de seleção for desmarcada.
Usar o Servidor de Administração como um servidor proxy da KSN	Se a caixa de seleção for marcada, o Kaspersky Endpoint Security usará o serviço Proxy da KSN. Você pode definir as configurações do serviço KSN Proxy nas propriedades do Servidor de Administração.
Usar servidores da Kaspersky Security Network se o servidor proxy da KSN não estiver disponível	Se a caixa de seleção for marcada, o Kaspersky Endpoint Security usará os servidores da KSN quando o serviço KSN Proxy estiver indisponível. Os servidores da KSN podem ser localizados no lado da Kaspersky e no lado de terceiros (quando a Kaspersky Private Security Network for usada).

Interação do usuário

Você pode definir as configurações da interface do aplicativo, bem como as configurações para a interação do aplicativo com o usuário de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo** → **Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Configurações gerais** → **Interação com o usuário**.
  5. Defina as configurações de interação do usuário.
  6. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Configurações adicionais → Interação do usuário**.
  5. Defina as configurações de interação do usuário.
  6. Salve suas alterações.

Configurações de interação do usuário

Configurações	Descrição
Iniciar o Kaspersky Endpoint Security durante a inicialização do computador (recomendado)	Se esta funcionalidade estiver ativada, o Kaspersky Endpoint Security será iniciado após o carregamento do sistema operacional, protegendo o computador durante a sessão inteira. Caso esta funcionalidade esteja desativada, o Kaspersky Endpoint Security não será iniciado após o carregamento do sistema operacional até que o usuário o inicie manualmente. A proteção do computador é desativada e os dados de usuário podem ser expostos a ameaças.
Mostrar o ícone do aplicativo	Esta caixa de seleção ativa/desativa a exibição do ícone do aplicativo na barra de menus em um computador remoto. Se essa caixa de seleção estiver marcada, o ícone do aplicativo será exibido na barra de menus. Se essa caixa de seleção estiver desmarcada, o ícone do aplicativo ficará oculto na barra de menus. Esta caixa de seleção está marcada por padrão.
Gerenciar atualizações localmente	Se essa caixa de seleção estiver marcada, o gerenciamento local das atualizações do Kaspersky Endpoint Security em um computador remoto será ativado. Se essa caixa de seleção estiver desmarcada, as atualizações do Kaspersky Endpoint Security em um computador remoto poderão ser gerenciadas apenas usando o plugin de administração do Kaspersky Endpoint Security no Kaspersky Security Center.
Gerenciar chaves localmente	Se a caixa de seleção estiver marcada, o gerenciamento local das chaves do Kaspersky Endpoint Security em um computador remoto será ativado. Se a caixa de seleção estiver desmarcada, as chaves do Kaspersky Endpoint Security em um computador remoto poderão ser gerenciadas apenas usando o plugin de administração do Kaspersky Endpoint Security no Kaspersky Security Center.
Sair do aplicativo	Se esta caixa de seleção estiver marcada, o comando **Sair** estará disponível no menu de contexto do ícone do aplicativo. O usuário pode sair do Kaspersky Endpoint Security no computador remoto. Se essa caixa de seleção estiver desmarcada, o comando **Sair** ficará indisponível no menu de contexto do ícone do aplicativo. O usuário não pode sair do Kaspersky Endpoint Security no computador remoto.

Autodefesa

É possível definir as configurações de Autodefesa de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.

4. Vá para **Configurações gerais** → **Autodefesa**.
5. Ative ou desative o componente usando o botão de alternância **Proteção por senha**.
6. Configure a Autodefesa.
7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Configurações adicionais** → **Interação do usuário**.
5. Ative ou desative o componente usando o botão de alternância **Proteção por senha**.
6. Configure a Proteção por senha.
7. Salve suas alterações.

Configurações de Autodefesa

Configurações	Descrição
Proteção por senha	Se o botão de alternância estiver ativado, o Kaspersky Endpoint Security solicitará uma senha ao usuário quando ele tentar executar uma operação que esteja dentro do escopo da Proteção por senha. O escopo de proteção por senha inclui operações proibidas (como desativar componentes de proteção) e as contas de usuário às quais o escopo de proteção por senha é aplicado. Depois que a Proteção por senha estiver ativada, o Kaspersky Endpoint Security solicitará a definição de uma senha para a conta KLAdmin.

Desempenho

É possível definir as configurações de desempenho de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Configurações gerais** → **Desempenho**.
5. Defina as configurações de desempenho.
6. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Configurações adicionais → Proteção**.
  5. Defina as configurações de desempenho.
  6. Salve suas alterações.

Configurações de desempenho

Configurações	Descrição
Adiar ou ignorar tarefas agendadas quando estiver em modo de bateria	Se esta funcionalidade estiver ativada, o Kaspersky Endpoint Security alternará para o modo de economia de energia. O Kaspersky Endpoint Security *cancela* tarefas agendadas. Você pode iniciar tarefas de verificação e de atualização manualmente, se necessário.
Limitar a utilização da CPU para tarefas de verificação	Para otimizar o desempenho do Kaspersky Endpoint Security, é possível limitar o consumo da CPU pela tarefa de verificação de malware. Se esta funcionalidade estiver ativada, a carga média em todos os núcleos da CPU da tarefa de verificação de malware se aproximará do valor especificado.

Relatórios e armazenamento

É possível definir as configurações dos Relatórios e armazenamento de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Configurações gerais → Relatórios e Armazenamento**.
  5. Defina as configurações de Relatórios e armazenamento.
  6. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.

3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Configurações adicionais → Relatórios e backup**.
5. Defina as configurações de Relatórios e armazenamento.
6. Salve suas alterações.

Configurações de Relatórios e armazenamento

Configurações	Descrição
Excluir relatórios após (dias)	Se a caixa de seleção estiver marcada, o prazo máximo de armazenamento do relatório será limitado ao intervalo de tempo definido. Após este período, o Kaspersky Endpoint Security exclui as entradas mais antigas do arquivo de relatório automaticamente.
Manter apenas eventos recentes	Se esta caixa de seleção for marcada, sempre que a tarefa for iniciada, o Kaspersky Endpoint Security excluirá informações sobre eventos não críticos que ocorreram desde o início anterior da tarefa, mas manterá notas importantes no relatório (por exemplo, informações sobre objetos maliciosos detectados).
Registrar eventos não críticos	Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security registrará os eventos não críticos no relatório (por exemplo, os eventos informacionais). Os eventos não críticos não afetam a proteção.
Excluir objetos após (dias)	Se a caixa de seleção estiver marcada, o prazo máximo de armazenamento do arquivo será limitado ao intervalo de tempo definido. Depois da expiração do período máximo de armazenamento, o Kaspersky Endpoint Security excluirá os arquivos mais antigos do Backup.

Configurações de rede

É possível definir as configurações de rede de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**
  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Configurações gerais → Configurações de rede**.
  5. Defina as configurações de rede.
  6. Salve suas alterações.
- **Uso do plug-in do Kaspersky Endpoint Security**
  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Configurações adicionais → Rede**.

5. Defina as configurações de rede.

6. Salve suas alterações.

Configurações de rede

Configurações	Descrição
Certificados raiz confiáveis	Lista de certificados raiz confiáveis. O Kaspersky Endpoint Security permite a instalação de certificados raiz confiáveis nos computadores dos usuários caso, por exemplo, seja necessário implementar um novo centro de certificação. O aplicativo permite adicionar um certificado para uma loja especial de certificado Kaspersky Endpoint Security. Neste caso, o certificado é considerado confiável somente para o aplicativo Kaspersky Endpoint Security. Em outras palavras, o usuário pode ter acesso a um site com um novo certificado no navegador. Caso outro aplicativo tente acessar o site, é possível ocorrer um erro de conexão devido a um problema de certificado.
Servidor proxy	Configurações do servidor proxy usadas por usuários de computadores clientes para acessarem a Internet. O Kaspersky Endpoint Security usa essas configurações para certos componentes de proteção, inclusive para atualizar bancos de dados e módulos do aplicativo.
Usar autenticação de servidor proxy	Se esta caixa de seleção estiver marcada, o aplicativo usa a autenticação com um nome de usuário e senha ao conectar-se ao servidor proxy.
Ignorar servidor proxy para endereços locais	Se a caixa de seleção for marcada, o Kaspersky Endpoint Security não usará um servidor proxy executando uma atualização de uma pasta compartilhada.
Verificação de conexões criptografadas	Esse recurso permite que os componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio e Controle da Web monitorem e manipulem conexões criptografadas (HTTPS).

Configurações de telemetria

É possível definir as configurações de telemetria de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.

  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.

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

  4. Vá para **Configurações gerais → Configurações de telemetria**.

  5. Defina as configurações de telemetria.

  6. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.

  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.

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

  4. Ir para **Configurações adicionais → Zona confiável → Configurações de telemetria**.

5. Defina as configurações de telemetria.

6. Salve suas alterações.

Configurações de telemetria

Configurações	Descrição
Telemetria do EDR Expert (on-premise)	**Importar** e **Exportar**. Você pode exportar as configurações de telemetria do EDR Expert (on-premise) para um arquivo JSON. Em seguida, será possível modificar o arquivo para, por exemplo, adicionar um grande número de IDs de eventos. Você também pode usar a função de exportação/importação para fazer backup das configurações de eventos enviados ou para migrar a lista para outra política.
Exclusões gerais	Para otimizar os dados transmitidos, você pode configurar regras de exclusão para determinados tipos de eventos. O Kaspersky Endpoint Security não coleta a telemetria que se enquadra nessa regra. Isso permite reduzir o tráfego e evitar o processamento de eventos de objetos e processos confiáveis.

Configurações do evento

Enquanto o aplicativo está em execução, vários *eventos* ocorrem. Eles podem ser puramente informativos ou conter informações críticas. Por exemplo, o aplicativo pode usar um evento para notificar sobre uma atualização bem-sucedida do banco de dados ou apontar um erro em um componente que precisa ser corrigido.

Os eventos do Kaspersky Endpoint Security podem ser classificados nas seguintes categorias de gravidade:

- *Eventos críticos* – eventos que apresentam uma ameaça perigosa à segurança do computador (detecção de objetos maliciosos, vulnerabilidades, problemas com o Kaspersky Endpoint Security). Os eventos críticos exigem sua atenção imediata. Recomendamos que você não desative as notificações sobre eventos críticos.

- *Falhas funcionais* são eventos que ocorrem quando o Kaspersky Endpoint Security funciona mal (erro de processamento, erro de configurações da tarefa). Esses eventos não ameaçam diretamente a segurança do computador, mas exigem sua intervenção para garantir que o Kaspersky Endpoint Security esteja funcionando corretamente e protegendo seus dispositivos.

- *Avisos* – eventos que não exigem a atenção imediata, mas que podem representar uma ameaça à segurança do computador no futuro.

- *Mensagens informativas* – eventos relatados para sua informação.

Independentemente de as notificações estarem ativadas ou desativadas, o Kaspersky Endpoint Security regista informações sobre todos os eventos do aplicativo nos relatórios do aplicativo.

Configurações de atualização

É possível definir as configurações de atualização de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.

  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.

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

  4. Vá para **Configurações gerais → Atualização**.

5. Definir as configurações de atualização.

6. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.

  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.

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

  4. Vá para a seção **Atualização**.

  5. Definir as configurações de atualização.

  6. Salve suas alterações.

Configurações de atualização

Configurações	Descrição
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. Se os servidores de atualização Kaspersky não estiverem disponíveis, o Kaspersky Endpoint Security poderá usar domínios alternativos para receber atualizações do banco de dados e do módulo do aplicativo. Para obter mais informações, consulte a Base de conhecimento do Suporte Técnico. A lista padrão de fontes de atualização inclui os servidores de atualização do Kaspersky Security Center e da Kaspersky. É possível adicionar outras fontes de atualização à lista. Você pode especificar servidores FTP ou HTTP e pastas compartilhadas como fontes de atualização. O Kaspersky Endpoint Security não oferece suporte as atualizações de servidores HTTPS, a menos que sejam servidores de atualização da Kaspersky. 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. Por padrão, o Kaspersky Endpoint Security usa o servidor do Kaspersky Security Center como a primeira fonte de atualização. Isso ajuda a conservar o tráfego durante a atualização. Se uma política não for aplicada ao computador, os servidores da Kaspersky serão selecionados como a primeira fonte de atualização nas configurações da tarefa local de Atualização, pois o aplicativo pode não ter acesso ao servidor do Kaspersky Security Center.

Agentes integrados

Configurar o Managed Detection and Response

É possível configurar o componente Managed Detection and Response de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo** → **Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Configuração de agentes integrados** → **Managed Detection and Response**.
  5. Ative ou desative o componente usando o botão de alternância **Managed Detection and Response**.
  6. Configure o componente Managed Detection and Response
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo** → **Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Detection and Response** > **Managed Detection and Response**.
  5. Ative ou desative o componente usando o botão de alternância **Managed Detection and Response**.
  6. Configure o componente Managed Detection and Response
  7. Salve suas alterações.

Configurações do componente Managed Detection and Response

Configurações	Descrição
Arquivo de configuração MDR	O arquivo BLOB contém o ID do cliente e informações sobre a licença do Kaspersky Managed Detection and Response. O arquivo BLOB está localizado no arquivo comprimido ZIP do arquivo de configuração do MDR. Você pode obter o arquivo comprimido ZIP no Kaspersky Managed Detection and Response Console. Para obter mais informações sobre um arquivo BLOB, consulte a Ajuda do Kaspersky Managed Detection and Response.

Configuração do Endpoint Detection and Response

É possível configurar o componente Endpoint Detection and Response de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Configuração de agentes integrados → Endpoint Detection and Response**.
  5. Ative ou desative o componente usando o botão de alternância **Managed Detection and Response**.
  6. Configure o componente Endpoint Detection and Response.
  7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.
     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para **Detection and Response** > **Endpoint Detection and Response**.
  5. Ative ou desative o componente usando o botão de alternância **Endpoint Detection and Response**.
  6. Configure o componente Endpoint Detection and Response.
  7. Salve suas alterações.

Configurações do Endpoint Detection and Response

Configurações	Descrição
Isolamento de rede	Isolamento automático do computador da rede em resposta a ameaças detectadas. Quando o isolamento de rede está ativado, o aplicativo corta todas as conexões ativas e bloqueia todas as novas conexões TCP/IP no computador. O aplicativo deixa apenas as seguintes conexões ativas: • Conexões listadas em Exclusões de isolamento de rede. • Conexões iniciadas pelos serviços do Kaspersky Endpoint Security. • Conexões iniciadas pelo Agente de Rede do Kaspersky Security Center.
Desbloquear automaticamente o dispositivo isolado em (horas)	O isolamento de rede pode ser desativado automaticamente após um tempo especificado ou manualmente.

Configurações	Descrição
Exclusões de isolamento de rede	Lista de regras para exclusões do isolamento de rede. As conexões de rede que correspondem às regras não são bloqueadas nos computadores quando o isolamento de rede está ativado. Para configurar as exclusões de isolamento de rede, é possível utilizar a lista de *perfis de rede padrão*. Por padrão, as exclusões incluem perfis de rede que contêm regras que garantem a operação ininterrupta de dispositivos com as funções de servidor DNS/DHCP e cliente DNS/DHCP. Você também pode modificar os ajustes de perfis de rede padrão ou definir as exclusões manualmente. As exclusões especificadas nas propriedades da política são aplicadas apenas se o isolamento de rede for ativado automaticamente em resposta a uma ameaça detectada. As exclusões especificadas nas propriedades do computador são aplicadas somente se o Isolamento de rede estiver ativado manualmente nas propriedades do computador no console do Kaspersky Security Center ou nos detalhes do alerta.
Prevenção de execução	Controle a execução de arquivos executáveis e scripts e abertura de arquivos de formato Office. Por exemplo, é possível impedir a execução de aplicativos considerados inseguros no computador selecionado. A prevenção de execução é compatível com um conjunto de extensões de arquivos do Office e um conjunto de interpretadores de script. Para usar o componente Prevenção de execução, você precisa adicionar regras de prevenção de execução.
Ação na execução ou abertura de objeto proibido	**Bloquear e adicionar ao log de eventos**. Nesse modo, o aplicativo bloqueia a execução de objetos ou a abertura de documentos que atendem aos critérios da regra de prevenção. O aplicativo também publica um evento sobre as tentativas de execução de objetos ou documentos abertos no log de eventos do sistema e no Kaspersky Security Center. **Adicionar ao log de eventos**. Neste modo, o Kaspersky Endpoint Security publica um evento sobre tentativas de execução de objetos executáveis ou documentos abertos que correspondem aos critérios da regra de prevenção no log de eventos do sistema e no Kaspersky Security Center, mas não bloqueia a tentativa de executar ou abrir o objeto ou documento. Este modo está marcado por padrão.
Regras de prevenção de execução	A *Regra de prevenção de execução* é um conjunto de critérios que o aplicativo leva em consideração ao reagir à execução de um objeto, por exemplo, ao bloquear a execução de um objeto. O aplicativo identifica arquivos por seus caminhos ou somas de verificação calculadas usando algoritmos de hash MD5 e SHA256.
Cloud Sandbox	*Cloud Sandbox* é uma tecnologia que permite detectar ameaças avançadas em um computador. O Kaspersky Endpoint Security encaminha automaticamente arquivos detectados para a Cloud Sandbox analisar. O Cloud Sandbox executa esses arquivos em um ambiente isolado para identificar atividades maliciosas e avaliar a sua reputação. Os dados nesses arquivos são então enviados para a Kaspersky Security Network. Portanto, caso o Cloud Sandbox detecte um arquivo malicioso, o Kaspersky Endpoint Security executará a ação apropriada para eliminar essa ameaça em todos os computadores em que esse arquivo for detectado. Uma conexão com a KSN é necessária para obter informações sobre os objetos que estão sendo analisados.

Configure o Endpoint Detection and Response Expert (on-premise)

É possível configurar o componente Endpoint Detection and Response Expert (on-premise) de uma das seguintes formas:

- **Usando o Plug-in de Proteção e Gerenciamento Unificado**

  1. Na janela principal do Web Console, selecione **Gerenciamento de ativo → Políticas**.
  2. Clique no nome da política do Kaspersky Endpoint Security.

     A janela de propriedades da política é aberta.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Vá para a seção **Configuração de agentes integrados → Endpoint Detection and Response Expert (on-premise)**.

5. Ative ou desative o componente usando o botão de alternância **Managed Detection and Response Expert (on-premise)**.
6. Configure o componente Managed Detection and Response Expert (on-premise)
7. Salve suas alterações.

- **Uso do plug-in do Kaspersky Endpoint Security**

1. Na janela principal do Web Console, selecione **Gerenciamento de ativo** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é aberta.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Detection and Response** > **Endpoint Detection and Response Expert (on-premise)**.
5. Ative ou desative o componente usando o botão de alternância **Managed Detection and Response Expert (on-premise)**.
6. Configure o componente Managed Detection and Response Expert (on-premise)
7. Salve suas alterações.

Configurações do componente Endpoint Detection and Response Expert (on-premise)

Configurações	Descrição
Solução Endpoint Detection and Response Expert	Soluções Endpoint Detection and Response Expert com as quais o Kaspersky Endpoint Security pode se integrar. • **Endpoint Detection and Response Expert (versão 7.1 ou anterior)** • **Endpoint Detection and Response Expert (versão 8.0 ou posterior)**
Configurações de conexão	Gerencie as seguintes configurações de conexão do servidor de coleta de telemetria ou KATA: • **Tempo limite de conexão do servidor**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor de Central Node diferente. • **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor do Central Node. É possível obter um certificado TLS no console do Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda do Kaspersky Anti Targeted Attack Platform). • **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um contêiner criptográfico é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console do Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda do Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha. O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner de criptografia com uma senha em branco.
Enviar solicitação de sincronização para o servidor a cada (min.) *(Disponível apenas para o Endpoint Detection and Response Expert versão 7.1 ou anterior)*	Frequência de solicitações de sincronização enviadas ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as configurações e tarefas modificadas do aplicativo.

Configurações	Descrição
Conexão com servidores KATA / Conexão com servidores de coleta de telemetria	Insira o endereço IP e a porta de conexão ao servidor do Kaspersky Anti Targeted Attack Platform ou ao servidor de coleta de telemetria. Você pode adicionar vários endereços do Central Node (para KATA) ou do servidor de coleta de telemetria. O Kaspersky Endpoint Security tenta se conectar ao servidor no primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar ao segundo endereço IP na lista e assim sucessivamente. As soluções EDR (KATA) e EDR Expert (on-premise) têm arquiteturas diferentes. Para o processamento de telemetria, o EDR Expert (on-premise) usa um servidor de coleta de telemetria e o EDR (KATA) usa um servidor do Central Node. Portanto, se você estiver integrando o aplicativo com o EDR Expert (on-premise), precisará adicionar um servidor de coleta de telemetria.
Enviar telemetria à KATA / Enviar telemetria aos servidores de coleta de telemetria	Essa função permite impedir completamente que a telemetria seja enviada ao servidor KATA ou ao servidor de coleta de telemetria, dependendo da solução selecionada. Por exemplo, se você estiver usando a Kaspersky Anti Targeted Attack Platform junto com outra solução que também utiliza telemetria, é possível desativar o envio de telemetria para a KATA (EDR). Isso permite otimizar a carga do servidor para essas soluções. Caso tenha a solução Managed Detection and Response e KATA (EDR) implantados, será possível usar a telemetria MDR e criar tarefas de Resposta a Ameaças no KATA (EDR).
Atraso máximo na transmissão de eventos (segundos)	O aplicativo sincroniza com o servidor para enviar eventos após expirar o intervalo de sincronização.
Ativar a limitação de solicitações	Esse recurso ajuda a otimizar a carga no computador. Caso a caixa de seleção esteja marcada, o aplicativo restringirá os eventos transmitidos. Caso o número de eventos exceda os limites configurados, o Kaspersky Endpoint Security interromperá o envio de eventos. **Número máximo de eventos por hora**. O aplicativo analisa o fluxo de dados de telemetria e restringe o envio de eventos caso ele exceda o limite de eventos configurado por hora. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. Caso o aplicativo esteja instalado em um servidor, o fluxo de dados de telemetria será maior. Para servidores, é recomendável aumentar o valor para 60 mil eventos por hora. **Porcentagem de excesso de limite de evento**. O aplicativo ordena os eventos por tipo (por exemplo, eventos "alterações no registro") e restringe a transmissão de eventos caso a proporção de eventos do mesmo tipo para o número total de eventos exceda o limite configurado em porcentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos torna-se volumosa o suficiente novamente.
Conexão com servidores de resposta *(Disponível apenas para o Endpoint Detection and Response Expert versão 8.0 ou posterior)*	Configurações de conexão com servidores de resposta. Insira o endereço IP do servidor de resposta (IPv4 ou IPv6) e a porta para conexão com o servidor. É possível adicionar vários endereços do servidor de resposta. O Kaspersky Endpoint Security tenta se conectar ao servidor no primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar ao segundo endereço IP na lista e assim sucessivamente.
Configurações de conexão *(Disponível apenas para o Endpoint Detection and Response Expert versão 8.0 ou posterior)*	Configure os seguintes itens para a conexão com o servidor de resposta: • **Tempo limite de conexão do servidor**. Tempo limite máximo de resposta do servidor de resposta. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta se conectar a um servidor de resposta diferente. • **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor de resposta. • **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor de resposta. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor de resposta, obter um contêiner de criptografia e definir uma senha para protegê-lo. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do servidor de resposta, é necessário também ativar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner de criptografia protegido por senha. O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner de criptografia com uma senha em branco.

Criar uma tarefa

Esta seção descreve como usar o Web Console e o Kaspersky Security Center Cloud Console para criar e configurar tarefas executadas pelo Kaspersky Endpoint Security em um computador cliente ou em um grupo de computadores gerenciados pelo Kaspersky Security Center.

Uma tarefa é um conjunto de ações configuráveis que o Kaspersky Endpoint Security executa em um computador cliente.

No Web Console e no Kaspersky Security Center Cloud Console, é possível criar as seguintes tarefas:

- Verificação
- Atualização
- Reversão
- Adicionar chave

Criar uma tarefa

1. Na seção **Dispositivos**, à esquerda, selecione a seção **Tarefas**.
2. Clique em **Adicionar**.
   O assistente para adicionar tarefas é iniciado.
3. Na lista suspensa **Aplicativo**, selecione **Kaspersky Endpoint Security for Mac 12.2.1**.
4. Na lista suspensa **Tipo de tarefa**, selecione a tarefa que deseja criar.
5. Se necessário, edite o nome da tarefa no campo **Nome da tarefa**.
6. Selecionar os dispositivos aos quais a tarefa será atribuída.
7. Defina configurações para o tipo de tarefa selecionado.
8. Conclua o assistente para adicionar tarefas clicando em **Concluir**.

> **Nota:** se você marcar a caixa de seleção **Abrir detalhes da tarefa quando a criação for concluída** na janela **Concluir a criação da tarefa**, poderá continuar com as modificações das configurações padrão da tarefa. Se você não marcar essa caixa de seleção, a tarefa será criada com as configurações padrão. É possível modificar as configurações padrão da tarefa posteriormente, a qualquer momento.

Você pode executar as seguintes ações nas tarefas:

- Iniciar e parar tarefas.
- Definir configurações de tarefas.
- Rastrear o progresso de uma tarefa.
- Copiar e mover tarefas de um grupo para outro.
- Excluir tarefas.

Para obter informações detalhadas sobre as tarefas do Kaspersky Security Center Web Console, consulte a ajuda do Kaspersky Security Center.

Para obter informações detalhadas sobre as tarefas do Kaspersky Security Center Cloud Console, consulte a ajuda do Kaspersky Security Center Cloud Console.

Definir as configurações da tarefa de Verificação

Na guia **Configurações do aplicativo**, é possível definir as configurações da tarefa de **Verificação** para o Kaspersky Endpoint Security em computadores remotos.

Abrir as configurações da Tarefa de Verificação

1. Vá para **Dispositivos** > **Tarefas**.
2. Clique duas vezes em uma tarefa com o tipo de tarefa **Verificação**.
3. Selecione a guia **Configurações do aplicativo**.

Faça o seguinte, se necessário:

- Defina um escopo da verificação.
- Especifique a ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto infectado.
- Selecione os tipos de arquivos que devem ser verificados pelo Kaspersky Endpoint Security ao executar a tarefa de Verificação.
- Defina as configurações de desempenho da verificação.
- Selecione os arquivos compostos que serão analisados pelo Kaspersky Endpoint Security.

Nota: o Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.

Definir as configurações da tarefa Adicionar chave

Na guia **Configurações do aplicativo**, é possível definir as configurações da tarefa **Adicionar chave** para o Kaspersky Endpoint Security em computadores remotos.

Abrir as configurações da tarefa Adicionar Chave

1. Vá para **Dispositivos** > **Tarefas**.
2. Clique duas vezes em uma tarefa com o tipo de tarefa **Adicionar chave**.
3. Selecione a guia **Configurações do aplicativo**.

Faça o seguinte, se necessário:

- Torne a chave de licença atual uma chave reserva.
- Selecione outra chave para ativar o Kaspersky Endpoint Security no computador de um usuário.
- Adicione uma nova chave de licença ao repositório do Kaspersky Security Center.

Configurar a tarefa de Atualização

Na guia **Configurações do aplicativo** é possível definir as configurações da tarefa de **Atualização** para o Kaspersky Endpoint Security em computadores remotos.

Abrir as configurações da Tarefa de Atualização

1. Vá para **Dispositivos** > **Tarefas**.
2. Clique duas vezes em uma tarefa com o tipo de tarefa **Atualização**.
3. Selecione a guia **Configurações do aplicativo**.

Os servidores de atualização Kaspersky dedicados são a principal fonte de atualização do Kaspersky Endpoint Security. O Kaspersky Endpoint Security também pode usar pontos de distribuição, pastas locais ou outros servidores da Web como *fonte de atualização*.

Se você gerenciar o Kaspersky Endpoint Security por meio do Kaspersky Security Center Web Console, a lista de fontes de atualização incluirá, por padrão, os Servidores de atualização Kaspersky e os servidores do Kaspersky Security Center. O Kaspersky Endpoint Security baixa as atualizações primeiro dos servidores do Kaspersky Security Center e depois dos Servidores de atualização Kaspersky.

Se você gerenciar o Kaspersky Endpoint Security por meio do Kaspersky Security Center Cloud Console, a lista de fontes de atualização incluirá, por padrão, os Servidores de atualização Kaspersky e os pontos de distribuição. O Kaspersky Endpoint Security baixa as atualizações primeiro dos pontos de distribuição e depois dos Servidores de atualização Kaspersky. Para obter informações detalhadas sobre os pontos de distribuição, consulte a ajuda do Kaspersky Security Center.

Faça o seguinte, se necessário:

- Ative ou desative a atualização dos módulos do aplicativo.
- Adicione ou exclua fontes de atualização que serão usadas para atualizar o Kaspersky Endpoint Security.

Obter uma chave de recuperação para uma unidade criptografada

Se um usuário de um computador cliente esquecer ou perder as suas credenciais e não puder acessar um disco criptografado, será possível obter uma chave de recuperação.

Obter uma chave de recuperação

1. Na janela principal do Kaspersky Security Center Web Console ou do Cloud Console, selecione **Configurações → Opções da interface**.
2. Ative o botão de alternância **Mostrar a criptografia e proteção de dados** para ativar o gerenciamento da criptografia de dados e clique em **Salvar**.

3. Vá para **Operações** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.

   A lista de dispositivos criptografados é exibida.

4. Marque a caixa de seleção ao lado do dispositivo com a unidade criptografada.

5. Clique em **Permitir acesso ao dispositivo em modo offline**.

6. Na caixa de diálogo **Permitir acesso ao dispositivo em modo offline**, selecione o plug-in da Web para o Kaspersky Endpoint Security e clique em **OK**.

7. Clique em **Obter chave de recuperação**.

   Uma chave de recuperação é exibida na janela de diálogo atual.

8. Salve a chave de recuperação do modo que considerar conveniente.

É possível usar essa chave de recuperação em um computador cliente para acessar a unidade criptografada.

Gerenciar o aplicativo pela linha de comando

Você pode gerenciar o aplicativo Kaspersky Endpoint Security a partir da linha de comando.

Nota: após a instalação das atualizações dos módulos do Kaspersky Endpoint Security, a versão do aplicativo cliente na linha de comando poderá ser diferente da versão instalada do aplicativo.

Sintaxe da linha de comando:

```
kav <comando> <parâmetros>
```

Cada comando tem um conjunto específico de parâmetros compatíveis.

Exibir a ajuda da linha de comando

Use o seguinte comando para exibir informações sobre a sintaxe da linha de comando do aplicativo:

```
kav -? | help
```

Executar verificação de malware

Sintaxe do comando:

```
kav scan <escopo da verificação> <ação> <tipos de arquivos> <exclusões> <parâmetros de relatório> <parâmetros avançados>
```

Nota: para executar uma verificação de malware, também é possível usar as tarefas criadas no aplicativo, ao iniciar uma tarefa a partir da linha de comando. A tarefa é iniciada com os parâmetros especificados na interface do Kaspersky Endpoint Security.

Descrição dos parâmetros

`<escopo da verificação>` – Este parâmetro especifica uma lista dos objetos que serão verificados em busca de código malicioso. É possível incluir vários parâmetros separados por um espaço.

Nota: o Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.

Os seguintes valores são possíveis:

- `<arquivos>` – Lista de caminhos dos arquivos e/ou pastas a serem verificados. Você pode especificar um caminho absoluto ou relativo para os arquivos. Os itens da lista são separados por um espaço.

  Nota: se o nome ou o caminho de um objeto incluir um espaço ou caracteres espaciais (como `$`, `&` ou `@`), o nome deverá ser colocado entre aspas simples (`' '`) ou cada um dos caracteres especiais deverá ser imediatamente precedido por uma barra invertida (`\`). Se for feita referência a uma pasta específica, todos os arquivos e subpastas nessa pasta serão verificados.

- `-all` – Verificação completa do computador.
- `-remdrives` – Todas as unidades removíveis.
- `-fixdrives` – Todas as unidades internas.
- `-netdrives` – Todas as unidades de rede.
- `-@:<arquivodelista.lst>` – Caminho para o arquivo que contém uma lista dos objetos e das pastas que fazem parte do escopo da verificação. O arquivo deve estar no formato de texto e cada objeto da verificação deve estar listado em uma linha separada. Somente pode ser inserido um caminho absoluto para o arquivo.

`<ação>` – Este parâmetro determina a ação a ser executada nos objetos maliciosos detectados durante a verificação. Se este parâmetro não for definido, a ação padrão será a ação correspondente ao valor `-i8`.

Os seguintes valores são possíveis:

- `-i0` – Nenhuma ação é executada no objeto, apenas informações sobre ele são salvas em um relatório.
- `-i1` – Os objetos são desinfectados ou ignorados, caso não seja possível desinfectá-los.
- `-i2` – Os objetos infectados são desinfectados ou excluídos, caso não seja possível desinfectá-los; os contêineres não são excluídos, exceto aqueles com cabeçalhos executáveis (arquivos SFX).
- `-i3` – Os objetos infectados são desinfectados ou excluídos, caso não seja possível desinfectá-los; os contêineres são completamente excluídos caso não seja possível excluir os arquivos infectados dentro deles.
- `-i4` – Os objetos infectados são excluídos; os contêineres são completamente excluídos caso não seja possível excluir os arquivos infectados dentro deles.
- `-i8` – Pergunta ao usuário qual ação deverá ser executada se um objeto infectado for detectado (opção usada por padrão).
- `-i9` – Pergunta ao usuário qual ação deverá ser executada após a conclusão da verificação.

`<tipos de arquivos>` – Este parâmetro define os tipos de arquivos que estão sujeitos à verificação de malware. Por padrão, se este parâmetro não for definido, somente arquivos potencialmente infectados (com base no conteúdo do arquivo) serão verificados.

Os seguintes valores são possíveis:

- `-fe` – Verifica somente os arquivos potencialmente infectados (com base na extensão do arquivo).
- `-fi` – Verifica somente os arquivos potencialmente infectados (com base no conteúdo do arquivo). Este parâmetro é usado por padrão.
- `-fa` – Verifica todos os arquivos.

`<exclusões>` – Este parâmetro define os objetos que serão excluídos da verificação. É possível incluir vários parâmetros separados por um espaço.

Os seguintes valores são possíveis:

- `-e:a` – Não verifica arquivos compactados.
- `-e:b` – Não verifica bancos de dados de e-mail.
- `-e:m` – Não verifica mensagens de e-mail em formato de texto.
- `-e:` `<máscara>` – Não verifica objetos por máscara.
- `-e:` `<segundos>` – Ignora objetos verificados por mais tempo do que a duração especificada (em segundos).
- `-es:` `<tamanho>` – Ignora objetos com um tamanho que excede o valor especificado (em MB).

`<parâmetros de relatório>` – Estes parâmetros definem o formato do relatório que contém os resultados da verificação. Você pode especificar um caminho absoluto ou relativo para o arquivo de relatório. Se este parâmetro não for definido, os resultados da reversão serão exibidos na tela mostrando todos os eventos.

Os seguintes valores são possíveis:

- `-r:` `<arquivo de relatório>` – Registra somente eventos importantes no arquivo de relatório especificado.
- `-ra:` `<arquivo de relatório>` – Registra todos os eventos no arquivo de relatório especificado.

`<parâmetros avançados>` – parâmetros que definem o uso de tecnologias de verificação de malware e arquivos de configuração:

- `-iSwift=<on|off>` – Ativa/desativa o uso do iSwift.
- `-c:` `<arquivo de configuração>` – defina o caminho para o arquivo de configuração que contém as configurações do aplicativo para a execução de tarefas de verificação de malware. Você pode especificar um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for especificado, os valores definidos na interface do aplicativo serão usados juntamente com os valores já especificados na linha de comando.

Exemplo:
Inicie a verificação das pastas ~/Documents, /Applications, e do arquivo chamado my test.exe:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Verificar os objetos listados no arquivo objects2scan.txt. Usar o arquivo de configuração scan_settings.txt. Ao concluir a verificação, criar um relatório de todos os eventos:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Um exemplo de arquivo de configuração:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

Atualizar o aplicativo

Sintaxe do comando:

```
kav update <fonte de atualização> <parâmetros de relatório> <parâmetros avançados>
```

Descrição dos parâmetros

`<origem da atualização>` – Um servidor HTTP ou uma rede/pasta local da qual as atualizações são baixadas. Se não for selecionado um caminho, a fonte de atualização será obtida nas configurações de atualização do aplicativo.

`<parâmetros de relatório>` – Estes parâmetros definem o formato do relatório que contém os resultados da verificação. Você pode especificar um caminho absoluto ou relativo para o arquivo de relatório. Se este parâmetro não for definido, os resultados da reversão serão exibidos na tela mostrando todos os eventos.

Os seguintes valores são possíveis:

- `-r: <arquivo de relatório>` – Registra somente eventos importantes no arquivo de relatório especificado.
- `-ra: <arquivo de relatório>` – Registra todos os eventos no arquivo de relatório especificado.

`<parâmetros avançados>` – Um parâmetro que define o uso de um arquivo de configuração.

`-c: <arquivo de configuração>` – Define o caminho para um arquivo de configuração que contém as configurações do aplicativo aplicadas ao atualizar o aplicativo. Você pode especificar um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for definido, serão usados os valores definidos na interface do aplicativo.

Exemplo:
Atualize os bancos de dados do aplicativo da fonte padrão, registrando todos os eventos no relatório:

```
kav update -ra:avbases_upd.txt
```

Atualize os módulos do Kaspersky Endpoint Security usando os parâmetros do arquivo de configuração updateapp.ini:

```
kav update -app=on -c:updateapp.ini
```

Reverter a última atualização

Sintaxe do comando:

```
kav rollback <parâmetros de relatório>
```

Importante: é necessário ter direitos de administrador para executar este comando.

Descrição dos parâmetros

`<parâmetros de relatório>` – Este parâmetro define o formato do relatório que contém os resultados da reversão da atualização. Você pode especificar um caminho absoluto ou relativo para o arquivo de relatório. Se este parâmetro não for definido, os resultados da reversão serão exibidos na tela mostrando todos os eventos.

Os seguintes valores são possíveis:

- `-r: <arquivo de relatório>` – Registra somente eventos importantes no arquivo de relatório especificado.
- `-ra: <arquivo de relatório>` – Registra todos os eventos no arquivo de relatório especificado.

Exemplo:
```
kav rollback -ra:rollback.txt
```

Iniciar/parar um componente ou uma tarefa

A sintaxe do comando de início:

```
kav start <nome da tarefa ou do componente> <parâmetros de relatório>
```

A sintaxe do comando de parada:

```
kav stop <nome da tarefa ou do componente>
```

Importante: é necessário ter direitos de administrador para executar o comando parar.

Descrição dos parâmetros

`<nome da tarefa ou do componente>` – Especifica um dos seguintes valores:

- `fm` ou `file_monitoring` – Proteção Contra Ameaças ao Arquivo
- `wm` ou `web_monitoring` – Proteção Contra Ameaças da Web
- `mail_monitoring` – Proteção Contra Ameaças ao Correio
- `ids` – Proteção Contra Ameaças à Rede
- `firewall` – Firewall
- `behaviordetection` – Detecção de Comportamento
- `exploitprevention` – Prevenção de Exploits
- `remediationengine` – Mecanismo de Remediação

- `devicecontrol` – Controle de dispositivos
- `webcontrol` – Controle da Web
- `full` ou `scan_my_computer` – Tarefa Verificação Completa
- `scan_objects` – Tarefa Verificação Personalizada
- `quick` ou `scan_critical_areas` – Tarefa Verificação Rápida
- `externalstoragesscanner` – Tarefa de Verificação de Disco Removível
- `updater` – Tarefa de atualização
- `rollback` – Tarefa de reversão
- `diskencryption` – Criptografia de disco FileVault
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response Expert (on-premise)
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

`<parâmetros de relatório>` – Esses parâmetros definem o formato do relatório de resultados da tarefa ou do componente. Você pode especificar um caminho absoluto ou relativo para o arquivo de relatório. Se este parâmetro não for definido, o Kaspersky Endpoint Security exibirá os resultados de acordo com os parâmetros configurados na interface do usuário.

Nota: `<parâmetros do relatório>` está disponível apenas para valores de `scan_objects`, `updater` e `rollback`.

Os seguintes valores são possíveis:

- `-r: <arquivo de relatório>` – Registra somente eventos importantes no arquivo de relatório especificado.
- `-ra: <arquivo de relatório>` – Registra todos os eventos no arquivo de relatório especificado.

Nota: as tarefas e os componentes iniciados no prompt de comando são executados com os parâmetros configurados na interface do usuário.

Exemplo:
Para ativar o componente Proteção Contra Ameaças ao Arquivo, digite o seguinte comando na linha de comando:

```
kav start fm
```

Para parar a tarefa Verificação Completa na linha de comando, digite o seguinte comando:

```
kav stop scan_my_computer
```

Exibir status e estatísticas de um componente ou de uma tarefa

A sintaxe do comando de:

```
kav status <nome da tarefa ou do componente>
```

A sintaxe do comando de estatísticas:

```
kav statistics <nome da tarefa ou do componente>
```

Descrição dos parâmetros

`<nome da tarefa ou do componente>` – Especifica um dos seguintes valores:

- `fm` ou `file_monitoring` – Proteção Contra Ameaças ao Arquivo
- `wm` ou `web_monitoring` – Proteção Contra Ameaças da Web
- `mail_monitoring` – Proteção Contra Ameaças ao Correio
- `ids` – Proteção Contra Ameaças à Rede
- `firewall` – Firewall
- `behaviordetection` – Detecção de Comportamento
- `exploitprevention` – Prevenção de Exploits
- `remediationengine` – Mecanismo de Remediação
- `devicecontrol` – Controle de dispositivos
- `webcontrol` – Controle da Web
- `full` ou `scan_my_computer` – Tarefa Verificação Completa
- `scan_objects` – Tarefa Verificação Personalizada
- `quick` ou `scan_critical_areas` – Tarefa Verificação Rápida
- `externalstoragesscanner` – Tarefa de Verificação de Disco Removível
- `updater` – Tarefa de atualização
- `rollback` – Tarefa de reversão
- `diskencryption` – Criptografia de disco FileVault

- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response Expert (on-premise)
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

Nota: se o comando de status for executado sem que um valor seja especificado para o parâmetro `<nome da tarefa ou do componente>`, o status de todos os componentes e tarefas do aplicativo será exibido. Para o comando de estatísticas, um valor deve ser especificado para o parâmetro `<nome da tarefa ou do componente>`.

Exportar as configurações de proteção

Sintaxe do comando:

```
kav export <nome da tarefa ou do componente> <arquivo para exportação>
```

Descrição dos parâmetros

`<nome da tarefa ou do componente>` – Especifica um dos seguintes valores:

- `fm` ou `file_monitoring` – Proteção Contra Ameaças ao Arquivo
- `wm` ou `web_monitoring` – Proteção Contra Ameaças da Web
- `mail_monitoring` – Proteção Contra Ameaças ao Correio
- `ids` – Proteção Contra Ameaças à Rede
- `firewall` – Firewall
- `behaviordetection` – Detecção de Comportamento
- `exploitprevention` – Prevenção de Exploits
- `remediationengine` – Mecanismo de Remediação
- `devicecontrol` – Controle de dispositivos
- `webcontrol` – Controle da Web
- `full` ou `scan_my_computer` – Tarefa Verificação Completa
- `scan_objects` – Tarefa Verificação Personalizada
- `quick` ou `scan_critical_areas` – Tarefa Verificação Rápida

- `externalstoragesscanner` – Tarefa de Verificação de Disco Removível
- `updater` – Tarefa de atualização
- `rollback` – Tarefa de reversão
- `diskencryption` – Criptografia de disco FileVault
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response Expert (on-premise)
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

`<arquivo de exportação>` – Caminho do arquivo para o qual as configurações do aplicativo são exportadas. Você pode especificar um caminho absoluto ou relativo para o arquivo.

Exemplo:
```
kav export fm fm_settings.txt
```

Ativar o aplicativo

Você pode ativar o Kaspersky Endpoint Security aplicando um arquivo de chave.

Sintaxe do comando:

```
kav license /add <arquivo de chave ou código de ativação da chave>
```

Descrição dos parâmetros

`<arquivo de chave>` - Arquivo de chave do aplicativo com extensão .key.

`<código de ativação da chave>` - Código de ativação no formato XXXX-XXXX-XXXX-XXXX.

Exemplo:
```
kav license /add ./1AA111A1.key
kav license /add A11A1-11111-1A1AA-1A11A
```

Instale a extensão do sistema

Sintaxe do comando:

```
kav activatesystemextension /sysext
```

Nota: Você precisa conceder as permissões ao Kaspersky Endpoint Security nas configurações de **Privacidade e Segurança** para finalizar a instalação da extensão.

Defina as conexões de rede

Você pode configurar as conexões de rede para os componentes da Proteção Contra Ameaças da Web e a Proteção Contra Ameaças à Rede.

Sintaxe do comando:

```
kav activatesystemextension /webav
```

Nota: Você precisa conceder as permissões ao Kaspersky Endpoint Security de filtragem de conteúdo da rede para finalizar a configuração.

Remover as chaves de licença

Você pode remover todas as chaves de licença atualmente adicionadas ao aplicativo.

Sintaxe do comando:

```
kav license /del
```

Importante: é necessário ter direitos de administrador para executar este comando.

Códigos de retorno da linha de comando

Os códigos gerais podem ser retornados por qualquer comando da linha de comando. Os códigos de retorno incluem códigos gerais e códigos específicos de uma determinada tarefa.

Sintaxe do comando para receber o código de retorno:

```
echo $?
```

Códigos de retorno gerais:

- `0` – Operação concluída com êxito
- `1` – Valor de parâmetro inválido

- `2` – Erro desconhecido
- `3` – Erro na conclusão da tarefa
- `4` – Tarefa cancelada

Códigos de retorno da tarefa de verificação de vírus:

- `101` – Todos os objetos maliciosos foram processados
- `102` – Objetos maliciosos detectados

Encerrar o aplicativo

Sintaxe do comando:

```
kav exit
```

Importante: é necessário ter direitos de administrador para executar este comando.

Desinstalar o aplicativo

Use a sequência de comandos abaixo para desinstalar o Kaspersky Endpoint Security usando a linha de comando:

```
sudo /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/UninstallScript
sudo /Library/Application\ Support/Kaspersky\ Lab/KAV/Binaries/UninstallScript
sudo rm -rf /Library/Application\ Support/Kaspersky\ Lab/ /Applications/Kaspersky
```

Importante: são necessários privilégios de administrador para desinstalar o aplicativo.

Comandos de gerenciamento de Detection and Response

Você pode usar a linha de comando para gerenciar a funcionalidade integrada da solução Detection and Response. Você pode gerenciar as soluções de Detection and Response se o gerenciamento usando o console do Kaspersky Security Center não for possível.

Gerenciar a prevenção de execução

Você pode exibir os ajustes de Prevenção de execução do computador cliente e desativar a Prevenção de execução no computador cliente.

Sintaxe do comando:

```
kav prevention </disable | /show>
```

Descrições dos comandos

`/disable` - O comando para desativar a Prevenção de execução no computador cliente.

`/show` - O comando para exibir os ajustes atuais de Prevenção de execução, incluindo o modo e a lista de regras de prevenção de execução.

Gerenciar o isolamento de rede

Você pode exibir os ajustes de isolamento de rede do host e desativar o isolamento de rede no host.

Sintaxe do comando:

```
kav isolation </off | /status>
```

Descrições dos comandos

`/off` - O comando para desativar o isolamento de rede.

Importante: é necessário ter direitos de administrador para executar este comando.

`/status` - O comando para exibir o status de isolamento de rede e as exclusões.

Nota: Esses comandos devem ser executados simultaneamente.

Entrar em contato com o Suporte Técnico

Essa seção descreve as formas para obter suporte técnico e os termos sob os ele está disponível.

Como obter Suporte Técnico

Caso não consiga encontrar uma solução para o seu problema na documentação do Kaspersky Endpoint Security ou em qualquer uma das fontes de informação sobre o Kaspersky Endpoint Security disponíveis, entre em contato com o Suporte Técnico. Os especialistas do Suporte Técnico responderão a todas as suas perguntas sobre a instalação e o uso do Kaspersky Endpoint Security.

Nota: a Kaspersky fornece suporte ao Kaspersky Endpoint Security durante seu ciclo de vida (consulte a página de ciclo de vida de suporte do aplicativo). Antes de entrar em contato com o Suporte Técnico, leia as regras de suporte.

Você pode entrar em contato com Suporte Técnico de uma das seguintes maneiras:

- Visitando o site de Suporte Técnico
- Enviando uma solicitação ao Suporte Técnico pelo portal Kaspersky CompanyAccount

Suporte Técnico via Kaspersky CompanyAccount

O Kaspersky CompanyAccount é um portal para empresas que usam aplicativos da Kaspersky. O portal Kaspersky CompanyAccount foi desenvolvido para facilitar a interação entre usuários e especialistas da Kaspersky por meio de solicitações on-line. Você pode usar o Kaspersky CompanyAccount para rastrear o status de suas solicitações on-line e também para armazenar um histórico delas.

Você pode registrar todos os funcionários da sua organização em uma única conta no Kaspersky CompanyAccount. Uma única conta permite gerenciar de modo centralizado as solicitações eletrônicas de funcionários registrados na Kaspersky, além de seus privilégios, por meio 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 de Suporte Técnico.

Adquirir informações para Suporte Técnico

Para o suporte e a resolução de problemas do aplicativo mais eficazes, os especialistas do Suporte Técnico podem solicitar que você altere temporariamente as configurações do aplicativo para fins de depuração durante o diagnóstico. Isso pode exigir que você faça o seguinte:

- Ative a funcionalidade que extrai informações de diagnóstico estendidas.
- Ajuste as configurações de componentes individuais do aplicativo que não estão disponíveis por meio dos elementos padrão da interface do usuário.
- Altere as configurações de transmissão de informações de diagnóstico extraídas.

Os especialistas do Suporte Técnico fornecerão todas as informações necessárias para executar as operações listadas e informarão sobre o escopo dos dados a serem adquiridos para fins de depuração. Depois que as informações de diagnóstico estendidas forem extraídas, elas serão salvas no computador do usuário. Os dados não serão enviados para a Kaspersky automaticamente.

Usar um arquivo de rastreamento

Depois de comunicar um problema aos especialistas de Suporte Técnico da Kaspersky, eles poderão solicitar que você gere um relatório com informações sobre o funcionamento do Kaspersky Endpoint Security e envie-o para o Suporte Técnico. Os especialistas do Suporte Técnico da Kaspersky também poderão solicitar a criação de um *arquivo de rastreamento*. O arquivo de rastreamento permite realizar um exame passo a passo da execução dos comandos do aplicativo e determinar quando ocorrem erros.

Criar um arquivo de rastreamento

O rastreio é um modo efetivo de registrar informações detalhadas sobre a atividade do aplicativo. Os especialistas do Suporte Técnico usam arquivos de rastreio para solucionar problemas.

Criar um arquivo de rastreamento

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Interface**, na seção **Rastros**, marque a caixa de seleção **Ativar rastreamento**.

Importante: recomendamos ativar o rastreamento apenas se solicitado por um especialista do Suporte Técnico da Kaspersky.

Os arquivos de rastreamento podem necessitar de muito espaço no disco. Quando você já não precisa de arquivos de rastreamento, desative o rastreamento.

Desativar o rastreio

1. Na barra de menus, clique no ícone do aplicativo e escolha **Ajustes**.

   É aberta a janela de ajustes do aplicativo.

2. Na guia **Interface**, na seção **Rastros**, desmarque a caixa de seleção **Ativar rastreamento**.

O Kaspersky Endpoint Security salva as seguintes informações em um arquivo de rastreamento:

- Informações sobre o dispositivo e o sistema operacional (ID exclusivo do dispositivo, tipo de dispositivo, endereços MAC dos dispositivos da rede, tipo de sistema operacional, versão do sistema operacional).
- Informações sobre a operação do aplicativo e os seus módulos.
- Informações sobre a assinatura (tipo de assinatura, região).
- Informações sobre a localidade de idioma, ID do aplicativo, personalização do aplicativo, versão do aplicativo, ID exclusivo de instalação do aplicativo, ID exclusivo do computador.
- Informações sobre o status da proteção antimalware do computador, bem como todos os objetos processados e detectados (nome do objeto detectado, data e a hora da detecção, endereço da Web a partir do qual ele foi baixado, nomes e tamanhos dos arquivos infectados e seus caminhos, endereço IP do computador que realizou o ataque e o número da porta do computador que era o alvo do ataque de rede, lista de atividades de malware e endereços da Web indesejados) e as decisões pertinentes tomadas pelo aplicativo e pelo usuário.
- Informações sobre aplicativos baixados pelo usuário (endereço da Web, atributos, tamanho do arquivo e informações sobre o processo que baixou o arquivo).
- Informações sobre os aplicativos iniciados e seus módulos (tamanho, atributos, data de criação, detalhes de cabeçalho PE, região, nome, local e empacotadores).
- Informações sobre erros e uso da interface do aplicativo da Kaspersky instalado.
- Informações sobre conexões de rede: endereço IP do computador remoto e do computador do usuário, números das portas através das quais a conexão foi estabelecida e o protocolo de rede da conexão.
- Informações sobre os pacotes de rede recebidos e enviados pelo computador pelas redes de TI e de telecomunicações.
- Informações sobre mensagens instantâneas e e-mails enviados e recebidos.
- Informações sobre endereços Web visitados: a hora em que a conexão foi estabelecida usando um protocolo aberto, dados de login e senha do site e o conteúdo dos cookies.
- Certificado público do servidor.

Os arquivos de rastreamento contêm apenas as informações necessárias para corrigir defeitos no aplicativo. A Kaspersky utiliza arquivos de rastreamento para investigar incidentes associados a erros na operação do aplicativo Kaspersky Endpoint Security.

Por padrão, a criação de arquivos de rastreamento é desativada. Você pode ativar a geração de arquivos de rastreamento nos ajustes do aplicativo.

Os arquivos de rastreamento só podem ser enviados manualmente à Kaspersky. O aplicativo não envia os arquivos de rastreamento à Kaspersky automaticamente.

É possível escolher como os arquivos de rastreamento são enviados à Kaspersky.

Antes de enviar arquivos de rastreamento à Kaspersky, revise os dados que eles contêm.

Importante: os arquivos de rastreamento podem conter informações pessoais ou sigilosas. Ao enviar arquivos de rastreamento à Kaspersky, você aceita fornecer todos os dados contidos neles e concorda com o método usado para enviá-los.

Fontes de informação sobre o aplicativo

Esta seção descreve as fontes de informações sobre o aplicativo.

É possível escolher a fonte de informação mais conveniente, dependendo da importância e urgência do problema que acontece.

Página do Kaspersky Endpoint Security no site da Kaspersky

Na página do Kaspersky Endpoint Security no site da Kaspersky, é possível visualizar informações gerais sobre o aplicativo, suas funções e recursos.

A página do Kaspersky Endpoint Security contém um link para a loja on-line. Uma vez na loja, é possível comprar ou renovar o aplicativo.

Página do Kaspersky Endpoint Security na Base de Conhecimento

A *Base de conhecimento* é uma seção do site de Suporte Técnico da Kaspersky.

Na página do Kaspersky Endpoint Security na Base de conhecimento, é possível ler artigos com informações úteis, recomendações e respostas a perguntas frequentes sobre como comprar, instalar e usar o aplicativo.

Os artigos da Base de conhecimento podem fornecer respostas às perguntas relacionadas ao Kaspersky Endpoint Security e a outros aplicativos da Kaspersky. Os artigos na Base de conhecimento também podem conter notícias sobre o Suporte Técnico da Kaspersky.

Acesse a Base de conhecimento a partir do menu suspenso Ajuda

1. Selecione **Ajuda** → **Suporte**.
2. Clique em **Suporte Técnico**.

Discussão sobre os aplicativos da Kaspersky em nosso 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.

No Fórum, é possível visualizar os tópicos de discussão, deixar seus comentários e criar novos tópicos de discussão.

Acessar o Fórum a partir do menu suspenso Ajuda

1. Selecione **Ajuda** → **Suporte**.
2. Clique em **Comunidade**.

Apêndices

Esta seção fornece informações que complementam o texto do documento.

Problemas e limitações conhecidos

O Kaspersky Endpoint Security tem os seguintes problemas e limitações conhecidos:

- Se um aplicativo que coleta informações e as envia para processamento estiver instalado no computador, o aplicativo Kaspersky Endpoint Security pode classificar esse aplicativo como malware. Para evitar isso, é possível excluir o aplicativo da verificação configurando o aplicativo Kaspersky Endpoint Security como descrito neste documento.
- As configurações funcionais do aplicativo podem ser modificadas ao editar os arquivos de configuração.
- No Kaspersky Security Center, tarefas locais podem ser listadas duas vezes nas propriedades de dispositivos gerenciados.
- Mudar a fonte de atualização para uma tarefa de atualização local desativa a execução automática da tarefa de atualização.
- Se você iniciar uma tarefa de reinicialização do computador usando o Console de Administração com uma mensagem para o usuário que contém um ponto e vírgula (;), a tarefa será exibida como concluída, mas o usuário não será solicitado a reiniciar o Mac.
- Para excluir o tráfego de rede do Safari da verificação pelo Kaspersky Endpoint Security, é necessário adicionar os seguintes caminhos à lista de exclusão:
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCServices/com.a`
  - `/System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com.apple.webkit`
- Para excluir o tráfego de rede do Google Chrome da verificação pelo Kaspersky Endpoint Security, é necessário adicionar o seguinte caminho à lista de exclusão:
  - `/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/<VersionNumber>/Helpers/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper`
- Depois de criar um perfil da política para uma política do Kaspersky Endpoint Security usando o Kaspersky Security Center Web Console e o Cloud Console, é necessário verificar se as configurações foram aplicadas corretamente nos computadores clientes.
- Ao ativar a criptografia de disco do FileVault nas configurações de política, os usuários com direitos de administrador podem descriptografar o disco de inicialização do Mac a partir das Configurações do Sistema (Preferências do Sistema).

- Alterações nas opções do servidor proxy serão aplicadas apenas após a reinicialização do Kaspersky Endpoint Security.
- O Safari pode não se conectar a um site com um certificado não confiável. É possível adicionar tais sites às exclusões ou usar outro navegador.
- Após desinstalar remotamente o Kaspersky Endpoint Security 11.2 ou posterior via Kaspersky Security Center, uma das extensões do sistema do aplicativo poderá permanecer na memória do computador. Depois disso, em casos raros, pode ocorrer um problema com a permissão acesso total ao disco ao instalar o Kaspersky Endpoint Security. Nesse caso, recomendamos desinstalar o aplicativo localmente e reinstalá-lo.
- Os aplicativos que precisam do Rosetta podem não ser instalados se o Kaspersky Endpoint Security estiver em execução. Para resolver o problema, saia do Kaspersky Endpoint Security e tente reinstalar o aplicativo.
- Os detalhes do alerta para ameaças detectadas em objetos compostos contêm informações somente sobre o próprio objeto detectado, sem um gráfico da cadeia de desenvolvimento de ameaças.
- Ao salvar uma senha para Proteção por senha, pode ocorrer um erro. Nesse caso, recomendamos desinstalar e reinstalar o aplicativo.
- O Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.
- Você não pode analisar um arquivo que foi colocado em quarentena pela tarefa Mover arquivo para a Quarentena.
- No Kaspersky Security Center, o nome do dispositivo é exibido corretamente somente se o nome NetBIOS, o nome do computador e o nome do host forem iguais.

Problemas corrigidos

A tabela abaixo lista todos os problemas descobertos em versões anteriores do Kaspersky Endpoint Security e corrigidos na versão atual.

Lista de problemas corrigidos na versão 12.2.1

ID do problema	Descrição do problema
10054891	Não é possível adicionar um aplicativo à Zona confiável na política do Kaspersky Endpoint Security for Mac no Web Console.

Lista de objetos verificados por extensão

Se, ao criar uma tarefa de verificação no Kaspersky Security Center, o usuário tiver selecionado a opção **Verificar aplicativos e documentos por extensão**, o Kaspersky Endpoint Security executará verificações de malware em objetos sem extensões e objetos com as seguintes extensões:

Formatos gerais:

- txt
- csv
- htm
- html

Arquivos multimídia (áudio/vídeo):

- flv
- f4v
- avi
- 3gp
- 3g2
- 3gp2
- 3p2
- divx
- mp4
- mkv
- mov
- qt
- asf
- wmv
- rm
- rmvb
- vob
- dat
- mpg

- mpeg
- bik
- fcs
- mp3
- mpeg3
- flac
- ape
- ogg
- aac
- m4a
- wma
- ac3
- wav
- mka
- rm
- ra
- ravb
- mid
- midi
- cda

Arquivos de imagem:

- jpg
- jpe
- jpeg
- jff
- gif

- png
- bmp
- tif
- tiff
- emf
- wmf
- eps
- psd
- cdr
- swf

Arquivos executáveis e de sistema:

- exe
- dll
- scr
- ocx
- com
- sys
- class
- o
- so
- elf
- prx
- vb
- vbs
- js
- bat

- cmd
- msi
- deb
- rpm
- sh
- pl
- dylib

Documentos e modelos:

- doc
- dot
- docx
- dotx
- docm
- dotm
- xsl
- xls
- xlsx
- xltx
- xlsm
- xltm
- xlam
- xlsb
- ppt
- pot
- pps
- pptx

- potx
- pptm
- potm
- ppsx
- ppsm
- rtf
- pdf
- msg
- eml
- vsd
- vss
- vst
- vdx
- vsx
- vtx
- xps
- oxps
- one
- onepkg
- xsn
- odt
- ods
- odp
- sxw
- pub
- mdb
- accdb
- accde

- accdr
- accdc
- chm
- mht

Arquivos comprimidos:

- zip
- 7z*
- 7-z
- rar
- iso
- cab
- jar
- bz
- bz2
- tbz
- tbz2
- gz
- tgz
- arj
- dmg
- smi
- img
- xar

Nota: o formato real de um arquivo pode não corresponder à extensão do nome do arquivo.

Máscaras nos caminhos para arquivos e pastas

Um nome de máscara de arquivo ou um nome de máscara de pasta representa o nome e a extensão de um arquivo ou o nome de uma pasta usando os símbolos comuns.

É possível usar os símbolos ao especificar o escopo de proteção e o escopo da verificação e a zona confiável:

- O símbolo til `~` substitui `/Usuários/<nome do usuário>` no caminho para o arquivo ou pasta. Por exemplo, o caminho `~/Mesa` significa que o escopo de proteção inclui pastas da `Mesa` de todos os usuários nos computadores que se deseja proteger.

- O símbolo de asterisco `*` substitui qualquer conjunto de caracteres no nome do arquivo ou pasta, exceto os caracteres `\` e `/` (os quais delimitam os nomes de arquivos e pastas nos caminhos para arquivos e pastas). Por exemplo, a máscara `/*/*.db*` incluirá todos os caminhos para os arquivos com uma extensão iniciando com `db` localizada nas pastas do disco interno, mas não em subpastas.

- Dois símbolos de asteriscos consecutivos `**` substituem qualquer conjunto de caracteres (inclusive um conjunto vazio) no nome do arquivo ou pasta, inclusive os caracteres `\` e `/` (os quais delimitam os nomes de arquivos e pastas nos caminhos para arquivos e pastas). Por exemplo, a máscara `/Folder/**/*.txt` incluirá todos os caminhos para os arquivos com a extensão `TXT` localizada na pasta denominada `Folder` e em suas subpastas. A máscara deve incluir pelo menos um nível de agrupamento. A máscara `/**/*.txt` não é uma máscara válida.

- O ponto de interrogação `?` substitui qualquer caractere único no nome do arquivo ou pasta, exceto os caracteres `\` e `/` (os quais delimitam os nomes de arquivos e pastas nos caminhos para arquivos e pastas). Por exemplo, a máscara `/Folder/???.txt` incluirá os caminhos para todos os arquivos localizados na pasta chamada `Folder` que possuem a extensão `TXT` e um nome composto por três caracteres.

Requisitos do arquivo IOC

Ao criar tarefas de Verificação IOC, considere os seguintes requisitos e limitações do arquivo IOC:

- O aplicativo é compatível com arquivos IOC com as extensões IOC, XML e JSON no padrão aberto OpenIOC versões 1.0 e 1.1 ou STIX versões 2.0 e 2.1 para descrever indicadores de comprometimento.

- Se, ao criar uma tarefa de Verificação de IOC na linha de comando, você carregar arquivos IOC, alguns dos quais não são compatíveis, quando a tarefa for executada, o aplicativo usará somente os arquivos IOC compatíveis. Se, ao criar uma tarefa de Verificação IOC na linha de comando, todos os arquivos IOC carregados não forem compatíveis, a tarefa ainda poderá ser executada, mas não detectará nenhum indicador de comprometimento. Não é possível fazer upload de arquivos IOC não compatíveis usando o Web Console ou o Cloud Console.

- Erros semânticos e termos e tags IOC não compatíveis em arquivos IOC não causam falha na execução da tarefa. Em tais seções de arquivos IOC, o aplicativo não detecta nenhuma correspondência.

- Os identificadores de todos os arquivos IOC usados em uma única tarefa de Verificação IOC devem ser exclusivos. Se houver arquivos IOC com o mesmo identificador, isso poderá afetar os resultados da execução da tarefa.

- Um único arquivo IOC não deve exceder 2 MB de tamanho. O uso de arquivos maiores fará com que as tarefas de Verificação de IOC sejam encerradas com um erro. O tamanho total de todos os arquivos adicionados à coleção IOC não deve exceder 10 MB. Se o tamanho total de todos os arquivos exceder 10 MB, será necessário dividir a coleção de IOC e criar várias tarefas de Verificação de IOC.

- Recomenda-se criar um arquivo IOC por ameaça. Isso facilita a análise dos resultados da tarefa de Verificação de IOC.

Os recursos e as limitações de compatibilidade do aplicativo com arquivos IOC são mostrados na tabela a seguir.

Recursos e limitações de compatibilidade para documentos IOC.

Condições compatíveis	OpenIOC 1.0:
	
	`is`
	`isnot` (como uma exceção do conjunto)
	`contains`
	`containsnot` não (como uma exceção do conjunto)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	STIX 2.0 e 2.1:
	
	`=`
	`!=`
	`>`
	`<`
	`=>`
	`<=`
	`in`
	`like`
	`matches`

Atributos de condição compatíveis	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Operadores compatíveis	`AND` `OR`
Tipos de dados compatíveis	`"date"`: data (condições aplicáveis: `is`, `greater-than`, `less-than`) `"int"`: integral (condições aplicáveis: `is`, `greater-than`, `less-than`) `"string"`: string (condições aplicáveis: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: duração em segundos (condições aplicáveis: `is`, `greater-than`, `less-than`)

Recursos de interpretação de tipo de dados	Os tipos de dados `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` são interpretados como string.
	
	O aplicativo é compatível com a interpretação do ajuste de `Content` para os tipos de dados `int` e `date` quando são definidos na forma de intervalos:
	
	OpenIOC 1.0:
	Usando o operador `TO` no campo `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Usando as condições `greater-than` e `less-than`
	Usando o operador `TO` no campo `Content`
	O aplicativo é compatível com a interpretação dos tipos de dados de `date` e `duration` se os indicadores estiverem configurados no formato `ISO 8601`, `Zulu Time Zone` e `UTC`.

Interpretadores de script compatíveis com a Prevenção de execução

A prevenção de execução é compatível com os seguintes interpretadores de script:

- PkgUtil
- PkgInstaller
- /usr/bin/osascript
- /usr/bin/osacompile
- /usr/local/bin/python
- /usr/local/bin/python3
- /usr/bin/perl
- /usr/bin/ruby
- /bin/bash
- /bin/zsh
- /bin/sh
- /bin/dash
- /bin/csh
- /bin/ksh
- /bin/tcsh

Importante: Se o script especificado na regra de prevenção de execução for aberto pelos interpretadores de script PkgUtil ou PkgInstaller já iniciados, a execução desse script não será bloqueada.

Como adicionar o certificado da Kaspersky Endpoint Security ao armazenamento de certificados do Mozilla Firefox

Se o navegador usar o armazenamento de certificados do Mozilla Firefox, você precisará exportar e adicionar o certificado da Kaspersky a esse armazenamento de certificados manualmente. Caso contrário, o navegador não poderá abrir páginas HTTPS.

Exporte o certificado da Kaspersky

1. Abra o **Launchpad** > **Outro** > **Acesso à Keychain** no Mac.
2. No painel esquerdo da janela, clique em **Sistema** e abra a guia **Certificados**.
3. Na lista de certificados, localize **Autoridade de certificação do antivírus Web da Kaspersky**.
4. Clique com o botão direito do mouse neste certificado e selecione **Exportar "Autoridade de certificação do antivírus Web da Kaspersky"**.
5. Selecione um local para salvar o certificado e clique em **Salvar**.

O certificado da Kaspersky será salvo.

Adicione o certificado da Kaspersky ao armazenamento de certificados do Mozilla Firefox

1. Abra o Mozilla Firefox
2. No canto superior direito, clique no botão de menu e selecione **Configurações**.
3. No painel esquerdo da janela, selecione **Privacidade e segurança**.
4. Role para baixo até a seção **Certificados**.
5. Clique em **Exibir certificados**.
6. Na janela exibida, clique em **Importar**.
7. Escolha o arquivo de certificado da Kaspersky e clique em **Abrir**.
8. Marque as caixas de seleção **Confiar nesta CA para identificar sites** e **Confiar nesta CA para identificar usuários de e-mail**. Clique em **OK**.

   O certificado da Kaspersky é importado para o armazenamento de certificados do Mozilla Firefox. Ele é exibido na lista de certificados na janela **Gerenciador de certificados**.

Importante: sempre que o aplicativo Kaspersky Endpoint Security é reinstalado, um novo certificado raiz do Kaspersky Endpoint Security é gerado. Isso significa que você precisa realizar esse procedimento após cada reinstalação do aplicativo Kaspersky Endpoint Security.

Configurações de rede para interação com serviços externos

O Kaspersky Endpoint Security usa as seguintes configurações de rede para interagir com serviços externos.

Endereço	Descrição
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocolo: `HTTPS` Porta: `443`	Ativar o aplicativo.

Endereço	Descrição

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protocolo: `HTTPS`
Porta: `443`
	Atualizar bancos de dados e módulos do software do aplicativo.

`downloads.upd.kaspersky.com` Protocolo: `HTTPS` Porta: `443`	• Atualizar bancos de dados e módulos do software do aplicativo. • Verificando o acesso aos servidores da Kaspersky. Se o acesso aos servidores que usam o sistema DNS não for possível, o aplicativo usará um DNS público. Isso é necessário para garantir que os bancos de dados de antivírus estejam atualizados e o nível de segurança para o computador seja mantido. O Kaspersky Endpoint Security usa a lista a seguir de servidores de DNS público na seguinte ordem: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168).

Endereço	Descrição
	Importante: as solicitações emitidas pelo aplicativo podem conter endereços de domínios e o endereço IP público do usuário porque o aplicativo estabelece uma conexão TCP/UDP com o servidor DNS. Essas informações são necessárias, por exemplo, para validar o certificado de um recurso da Web ao usar HTTPS. Se o Kaspersky Endpoint Security usar um servidor DNS público, o processamento de dados seguirá a política de privacidade do serviço correspondente. **Como impedir que o Kaspersky Endpoint Security use um servidor DNS público** 1. Saia do aplicativo Kaspersky Endpoint Security no dispositivo do usuário. 2. Adicione a variável `ForceUseSystemDNS` e defina o valor como `1` no arquivo de configuração do aplicativo Kaspersky Endpoint Security localizado em `/Library/Application Support/Kaspersky Lab/KAV/Binaries/config.xml`. 3. Inicie o aplicativo Kaspersky Endpoint Security. Como resultado, o aplicativo Kaspersky Endpoint Security usará apenas o DNS do sistema.
`touch.kaspersky.com` Protocolo: `HTTP`	• Recebimento do tempo confiável para verificar o período de validade do certificado (conexão TLS). • Aviso sobre o acesso negado a um recurso da Web no navegador quando a Proteção Contra Ameaças da Web estiver em execução.

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protocolo: `HTTP`
Porta: `80`
	Atualizar bancos de dados e módulos do software do aplicativo.

Endereço	Descrição

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protocolo: `HTTPS`
Porta: `443`
	Usar a Kaspersky Security Network.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protocolo: `KSN`
Porta: `443`, `1443`
	Usar a Kaspersky Security Network.

`click.kaspersky.com`
 	
`redirect.kaspersky.com`
Protocolo: `HTTPS`
Porta: `443`
	Siga os links da interface.

Configurações usadas para criptografia

Endereço	Descrição

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocolo: `HTTP`
Porta: `80`
	Infraestrutura de chave pública (PKI).

Informações sobre código de terceiros

As informações sobre códigos de terceiros estão contidas no arquivo legal_notices.txt, na pasta de instalação do aplicativo.

Notas sobre marcas comerciais

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

ActiveSync, Active Directory, Excel, IIS, Microsoft, Outlook, Windows, Windows Installer e WMI são marcas comerciais do grupo de empresas da Microsoft.

Apple, Apple Remote Desktop, FileVault, iCloud, Keychain, Launchpad, Mac, macOS, Rosetta, Safari e Xcode são marcas comerciais registradas da Apple Inc.

Chrome, Gmail, Google e Google Chrome são marcas registradas da Google LLC.

Composer e JAMF são marcas registradas ou de direito comum da JAMF SOFTWARE, LLC nos Estados Unidos e em outros países.

Firefox, Mozilla e Thunderbird são marcas comerciais registradas da Mozilla Foundation nos Estados Unidos e em outros países.

Intel é uma marca comercial da Intel Corporation ou de suas subsidiárias.

JavaScript é uma marca comercial registrada da Oracle e/ou suas afiliadas.

Linux é a marca registrada de Linus Torvalds nos Estados Unidos e outros países.

Parallels, o logotipo da Parallels e Coherence são marcas comerciais ou marcas registradas da Parallels International GmbH.

VMware e VMware Fusion são marcas comerciais ou registradas da VMware, Inc. nos Estados Unidos e em outros países.

A janela Suporte ao usuário

Esta janela fornece as seguintes informações:

- Versão do Kaspersky Endpoint Security
- Data de lançamento dos bancos de dados atualmente usados pelo Kaspersky Endpoint Security
- Versão do sistema operacional instalado no computador

Suporte Técnico

Clique nesse botão para abrir a Base de conhecimento do Suporte Técnico da Kaspersky, onde será possível encontrar artigos sobre o Kaspersky Endpoint Security publicados por especialistas da Kaspersky.

Comunidade

Clicar nesse botão abre a comunidade na qual é possível discutir sobre o Kaspersky Endpoint Security com especialistas da Kaspersky e outros usuários.

Fechar

Clique neste botão para fechar a janela de suporte ao usuário.

A janela Configurações de certificado

Na guia **Geral**, você pode selecionar o armazenamento de certificado para verificar o tráfego HTTPS criptografado no navegador Mozilla Firefox:

- **Chaves Raízes do Sistema (recomendado)**
- **Armazenamento de certificados nas configurações do navegador Mozilla Firefox**

  Nesse caso, será necessário adicionar manualmente o certificado do Kaspersky Endpoint Security ao armazenamento de certificados do navegador Mozilla Firefox. Para obter mais informações, consulte Como adicionar o certificado da Kaspersky Endpoint Security ao armazenamento de certificados do Mozilla Firefox.

Na guia **Certificados confiáveis**, é possível criar uma lista de certificados raiz confiáveis para conectar-se aos servidores correspondentes sem exibir notificações.

Por padrão, a lista está vazia.

+

Clicar nesse botão abre um diálogo para adicionar certificados que serão considerados confiáveis.

–

Clicar nesse botão remove o certificado selecionado da lista de certificados confiáveis.

Nome do Certificado

Essa coluna exibe os nomes dos certificados raiz confiáveis.

Cancelar

Clicar nesse botão fecha a janela sem salvar as mudanças.

Salvar

Clicar nesse botão salva a lista atual de certificados raiz confiáveis e fecha a janela.

A janela Verificar certificado

Exibir Certificado

Clicar nesse botão abre uma janela do sistema com informações sobre o certificado.

Cancelar

Clicar nesse botão fechar a janela.

Adicionar em Confiável

Clicar nesse botão adiciona o certificado na lista de certificados confiáveis. Assim, será possível conectar ao servidor correspondente sem receber notificações.

Conectar

Clicar nesse botão conecta o usuário ao servidor.

Nota: os botões disponíveis podem variar de acordo com o tipo de certificado.

A janela Selecionar certificado

Lista de certificados disponíveis

Marque a caixa de seleção ao lado de um certificado para usá-lo ao se conectar ao servidor.

Exibir Certificado

Clicar nesse botão abre uma janela do sistema com informações sobre o certificado.

Cancelar

Clicar nesse botão fechar a janela.

Continuar

Ao clicar nesse botão, a conexão com o servidor continua usando o certificado selecionado.

A janela “Arquivo comprimido protegido por senha detectado”

Caso o Kaspersky Endpoint Security precise verificar um arquivo comprimido protegido por senha enquanto a Proteção Contra Ameaças ao Arquivo ou uma tarefa de verificação estiver em execução, uma janela de notificações será exibida.

Arquivo comprimido

Caminho ao arquivo.

Senha

Campo para inserir a senha.

Caso insira a senha, o Kaspersky Endpoint Security verificará o arquivo comprimido em busca de malware e outras ameaças à segurança do computador.

Ignorar arquivos protegidos

Se você clicar nesse botão, o objeto e todos os objetos do mesmo tipo serão ignorados.

Ignorar

Se você clicar nesse botão, o objeto será ignorado.

A caixa de diálogo Objeto detectado

Quando o Kaspersky Endpoint Security detecta um vírus ou outra ameaça à segurança do computador, uma janela de notificações é exibida na tela.

Detectado(a)

O nome do objeto de acordo com a classificação da Virus Encyclopedia da Kaspersky.

Detalhes

Clicar nesse botão abre uma página na Virus Encyclopedia da Kaspersky com informações sobre o objeto detectado.

Objeto

Caminho para a pasta com o objeto detectado ou o endereço da Web onde o objeto foi detectado.

Aplicar a todos

Essa caixa de seleção ativa/desativa a ação selecionada para todos os objetos do mesmo tipo durante a sessão atual da Proteção Contra Ameaças ao Arquivo, Proteção Contra Ameaças da Web ou de uma tarefa de verificação de malware.

Essa caixa de seleção vem desmarcada por padrão.

A sessão atual da Proteção Contra Ameaças ao Arquivo ou da proteção Contra Ameaças da Web é definida como o tempo desde que o componente foi iniciado até ser interrompido, ou até que o aplicativo seja encerrado ou reiniciado. A sessão atual de tarefas de verificação de malware é definida como o tempo desde o início de uma tarefa de verificação de malware até a sua conclusão.

Os botões com as ações que podem ser executadas nos objetos detectados variam dependendo do tipo de objeto detectado.

Você pode selecionar uma das seguintes ações:

- **Desinfectar**. Desinfeta o objeto. Antes de executar a desinfecção, o Kaspersky Endpoint Security cria uma cópia de backup do arquivo, caso você precise restaurar o arquivo original.
- **Excluir**. Exclui o objeto. Antes de executar a exclusão, o Kaspersky Endpoint Security cria uma cópia de backup do arquivo, caso você precise restaurar o arquivo original.
- **Não bloquear**. Permite o acesso a um site considerado um objeto de tráfego da Web perigoso.
- **Bloquear**. Nega o acesso a um site considerado um objeto de tráfego da Web perigoso.
- **Excluir arquivo comprimido**. Exclui o arquivo que contém o objeto detectado.
- **Ignorar arquivos protegidos**. Ignora os arquivos comprimidos protegidos por senha durante as verificações de malware.
- **Ignorar**. Bloqueia o acesso ao objeto, mas não realiza ações nele.

A janela “Verificação”



Clicar neste botão lhe leva de voltar à janela anterior do Kaspersky Endpoint Security.



Clicar neste botão lhe leva adiante para a próxima janela do Kaspersky Endpoint Security.



Clicar neste botão exclui todos os registros de todas as tarefas de verificação de malware na janela **Verificação**.

Agendar a verificação

Clicar neste botão abre uma caixa de diálogo onde você pode agendar tarefas de Verificação Rápida ou Verificação Completa.

Verificação rápida

Clicar no botão Iniciar ( ) nesta seção executa uma tarefa de Verificação Rápida.

Verificação completa

Clicar no botão Iniciar ( ) nesta seção executa uma tarefa de Verificação Completa.

Clicar neste botão interrompe a tarefa de verificação de malware selecionada.

Este botão será exibido se uma tarefa de verificação de malware estiver em execução.

Ajustes

Clicar nesse botão abre a guia **Verificação**, em que é possível configurar as tarefas de verificação.

Escolher

Clicar neste botão abre uma caixa de diálogo onde você pode selecionar um arquivo ou pasta para verificar.

Na parte inferior da seção **Arquivos e pastas**, é possível ver os registros de todas as tarefas de verificação de malware que foram executadas para arquivos ou pastas escolhidas.

Detalhes

Clicar neste botão abre a janela do relatório da tarefa de verificação de malware.

Esse botão é exibido quando você passa o cursor do mouse sobre uma tarefa de verificação.

Limpar histórico de verificação

Clicar nesse botão exclui todos os registros de todas as tarefas de verificação de malware.

Mostrar tudo

Ao clicar neste botão, a janela **Objetos detectados** é aberta, onde será possível visualizar todos os objetos detectados.

Nota: o Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.

A janela Objetos detectados

A seção **Objetos detectados** contém objetos maliciosos detectados pelo Kaspersky Endpoint Security.

Desinfectar tudo

Clique neste botão para iniciar a desinfecção de todos os objetos maliciosos detectados que foram detectados.

Ignorar tudo

Ao clicar neste botão, todos os objetos maliciosos da lista de objetos maliciosos na seção **Objetos detectados** são removidos.

•••

Clique neste botão para exibir uma lista suspensa onde você pode selecionar uma das seguintes ações para ser executada com um objeto malicioso:

- **Desinfectar**. Desinfeta o objeto. Antes da desinfecção, o aplicativo Kaspersky Endpoint Security cria uma cópia de backup do arquivo para que ele possa ser restaurado ou desinfectado posteriormente sem o risco de perda de dados.
- **Ignorar**. Remove o objeto da lista de objetos detectados.

A seção **Outros objetos** contém objetos detectados que não são maliciosos, mas que podem ser usados por invasores para danificar o computador ou os dados.

Excluir tudo

Clicar nesse botão exclui todos os objetos detectados do computador.

Ignorar tudo

Ao clicar neste botão, todos os objetos detectados da lista de objetos detectados na seção **Outros objetos** são removidos.

•••

Clique neste botão para exibir uma lista suspensa onde você pode selecionar uma das seguintes ações para ser executada com um objeto detectado:

- **Excluir**. Exclui o objeto detectado do computador.
- **Ignorar**. Remove o objeto da lista de objetos detectados.

A seção **Efetuar backup** contém cópias de backup dos objetos detectados.

Excluir tudo

Clicar nesse botão exclui todas as cópias de backup dos objetos detectados do computador.

•••

Clique neste botão para exibir um menu suspenso onde você pode selecionar uma das seguintes ações para ser executada com um objeto do backup:

- **Excluir cópia de backup**. Exclui a cópia de backup do objeto detectado do computador.
- **Restaurar o arquivo**. Restaura a cópia de backup do arquivo selecionado na lista para o local original com o mesmo nome que o arquivo original tinha antes da desinfecção ou exclusão. Se um objeto com o mesmo nome já existir no local original (por exemplo, se o Kaspersky Endpoint Security tiver criado uma cópia do arquivo original antes da desinfecção ou de ter desinfectado o arquivo original), um aviso será exibido. Você pode alterar o local do objeto que está sendo restaurado ou renomeá-lo.

A janela Licença



Clicar neste botão lhe leva de voltar à janela anterior do Kaspersky Endpoint Security.



Clicar neste botão lhe leva adiante para a próxima janela do Kaspersky Endpoint Security.

Nota: esta janela varia dependendo de o Kaspersky Endpoint Security estar ativado e do tipo de licença ou assinatura usada.

Esta janela pode conter as seguintes informações:

- Status da licença ou assinatura
- Chaves ativas
- Chaves reservas (caso existam)
- O tipo de licença e o número de computadores nos quais é possível usar o aplicativo com a licença ou assinatura atual
- Recursos do aplicativo que estão disponíveis na licença ou assinatura atual
- Data e hora de expiração da licença
- Número de dias até a licença expirar

Nesta janela, você pode executar as seguintes ações:

- Ativar o aplicativo inserindo um código de ativação.
- Acesse um site com informações sobre como comprar uma licença na loja on-line da Kaspersky.
- Abrir o site do fornecedor do Kaspersky Endpoint Security com as informações sobre renovação de assinatura.
- Atualizar o status da sua assinatura.

Para obter mais informações sobre as licenças do Kaspersky Endpoint Security, entre em contato com o administrador de sistemas em sua organização.

Janela Escopo da proteção

Na seção **Escopo da proteção**, é possível visualizar e editar o escopo da proteção.

Todos os discos removíveis

Esta caixa de seleção ativa/desativa a proteção em tempo real de todas os discos removíveis.

Essa caixa de seleção está marcada por padrão.

Todos os discos internos

Essa caixa de seleção ativa/desativa a proteção em tempo real de todas os discos internos.

Essa caixa de seleção está marcada por padrão.

Todos os discos de rede

Essa caixa de seleção ativa/desativa a proteção em tempo real de todas as unidades de disco da rede.

Essa caixa de seleção está marcada por padrão.

+

Clicar nesse botão abre uma lista onde você pode selecionar um item para criar o escopo de proteção:

- **Arquivos e pastas**. Selecionar esse item abre uma caixa de diálogo para adicionar um arquivo ou uma pasta ao escopo de proteção.
- **Todos os discos**. Ao selecionar este item, todos os discos removíveis, os discos internos, e os discos de rede do computador são adicionados ao escopo da proteção.
- **Todos os discos removíveis**. Ao selecionar este item, todas os discos removíveis do computador são adicionados ao escopo de proteção.
- **Todos os discos internos**. Selecionar esse item adiciona todos os discos internos do computador ao escopo de proteção.
- **Todos os discos de rede**. Selecionar esse item adiciona todas as unidades de rede do computador ao escopo de proteção.
- **Memória**. Selecionar esse item adiciona a memória do computador ao escopo de proteção.
- **Objetos da inicialização**. Selecionar esse item adiciona todos os arquivos executáveis iniciados na inicialização do sistema operacional ao escopo de proteção. A verificação de objetos de inicialização torna possível detectar rootkits.

A caixa de seleção ao lado de um item da lista ativa/desativa a proteção em tempo real dos objetos associados a esse item.

–

Clicar nesse botão exclui o item selecionado da lista de escopo de proteção.

Por padrão, os itens incluídos na lista do escopo de proteção não podem ser removidos.

Na seção **Otimização**, é possível configurar se o Kaspersky Endpoint Security verifica o volume do sistema somente leitura.

Ignorar a verificação de volumes de sistema somente leitura

Esta caixa de seleção ativa/desativa a verificação do volume do sistema somente leitura pelo Kaspersky Endpoint Security.

Essa caixa de seleção está marcada por padrão.

Importante: a otimização pode estar desativada por motivos de segurança.

Janela Escopo de verificação

Nessa janela, você pode ver e editar o escopo de verificação da tarefa Verificação Rápida.

A caixa de seleção ao lado de um objeto na lista ativa/desativa a verificação desse objeto.

+

Clicar nesse botão abre uma lista para ajustar o escopo de verificação:

- **Arquivos e pastas**. Selecionar esse item abre uma caixa de diálogo para adicionar um arquivo ou uma pasta ao escopo de verificação.
- **Todos os discos**. Ao selecionar esse item, todos os discos removíveis, internos e discos de rede do computador são adicionados ao escopo da verificação.
- **Todos os discos externos**. Ao selecionar esse item, todos os discos removíveis do computador são adicionados ao escopo da verificação.
- **Todos os discos internos**. Selecionar esse item adiciona todos os discos internos do computador ao escopo de verificação.
- **Todos os discos de rede**. Selecionar esse item adiciona todas as unidades de rede do computador ao escopo de verificação.
- **Memória**. Selecionar esse item adiciona a memória do computador ao escopo de verificação.
- **Objetos da inicialização**. Selecionar esse item adiciona todos os arquivos executáveis iniciados na inicialização do sistema operacional ao escopo de verificação. A verificação de objetos de inicialização torna possível detectar rootkits.

–

Clicar nesse botão remove o item selecionado da lista de escopo de verificação.

Por padrão, os itens incluídos na lista do escopo de verificação não podem ser removidos.

Na seção **Otimização**, é possível configurar se o aplicativo da Kaspersky Endpoint Security verificará o volume do sistema somente leitura ao executar uma tarefa de verificação.

Ignorar a verificação de volumes de sistema somente leitura

Esta caixa de seleção ativa/desativa a verificação do volume do sistema somente leitura pelo Kaspersky Endpoint Security.

Caso esta caixa de seleção esteja marcada, o Kaspersky Endpoint Security não verificará o volume do sistema em somente leitura. Isso reduz significativamente o tempo de verificação.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará o volume do sistema somente leitura.

Esta caixa de seleção está marcada por padrão.

Nota: o Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.

A guia Essencial

Na seção **Geral**, é possível ativar ou desativar a proteção do computador contra malware e outras ameaças à segurança do computador.

Ativar proteção

Esta caixa de seleção ativa/desativa a proteção em tempo real contra malware e outras ameaças à segurança do computador.

Essa caixa de seleção está marcada por padrão.

Verificar conexões seguras (HTTPS)

Essa caixa de seleção ativa/desativa a verificação de conexões criptografadas (HTTPS) pelo Kaspersky Endpoint Security e a exibição de notificações quando o Controle da Web bloqueia o acesso do usuário a recursos perigosos da Web.

Essa caixa de seleção vem desmarcada por padrão.

Zona Confiável

Clicar nesse botão abre uma janela onde você pode editar a Zona Confiável criando uma lista de objetos nos quais você confia e não deseja verificar se há malware.

Ajustes

Clicar neste botão abre a janela onde você pode gerenciar a lista de certificados raízes confiáveis e selecionar o armazenamento de certificados para verificar o tráfego HTTPS criptografado no navegador Mozilla Firefox.

Na seção **Proteção Contra Ameaças ao Arquivo**, é possível ativar ou desativar a Proteção Contra Ameaças ao Arquivo e selecionar a ação que o Kaspersky Endpoint Security executará ao detectar um arquivo infectado.

Ativar Proteção Contra Ameaças ao Arquivo

Esta caixa de seleção ativa/desativa a Proteção Contra Ameaças ao Arquivo.

Essa caixa de seleção está marcada por padrão.

Escopo da proteção

Clicar neste botão abre uma janela onde você pode criar o escopo de proteção.

Desinfectar ou excluir objetos maliciosos automaticamente

O Kaspersky Endpoint Security bloqueia o acesso ao arquivo infectado e tenta desinfectá-lo sem solicitar a confirmação do usuário. Antes de executar a desinfecção, o Kaspersky Endpoint Security salva uma cópia de backup do arquivo no Backup. Se a desinfecção for bem-sucedida, o Kaspersky Endpoint Security salvará o arquivo em sua localização original com o nome original do arquivo. Se ocorrer falha na desinfecção, o Kaspersky Endpoint Security manterá o arquivo infectado bloqueado e em sua localização original. As informações sobre a detecção do objeto infectado são registradas no relatório **Objetos processados**.

Perguntar o que fazer

O Kaspersky Endpoint Security exibe uma janela de notificações com informações sobre o objeto malicioso suspeito de infectar o arquivo e solicita que você escolha a ação a ser executada pelo Kaspersky Endpoint Security. As ações disponíveis podem variar dependendo do status do objeto.

Esta ação está selecionada por padrão.

Na seção **Proteção Contra Ameaças da Web**, é possível ativar ou desativar a Proteção Contra Ameaças da Web e selecionar a ação que o Kaspersky Endpoint Security deve executar quando detectar objetos perigosos no tráfego na Web.

Ativar Proteção Contra Ameaças da Web

Esta caixa de seleção ativa/desativa a Proteção Contra Ameaças da Web.

Essa caixa de seleção está marcada por padrão.

Bloquear objetos perigosos de tráfego da Web automaticamente

O Kaspersky Endpoint Security bloqueia o acesso ao site no qual um objeto de tráfego da Web perigoso foi detectado sem solicitar confirmação.

Perguntar o que fazer

O Kaspersky Endpoint Security exibe uma janela de notificações com informações sobre o objeto de tráfego da Web detectado e solicita que você escolha a ação a ser executada. As ações disponíveis podem variar dependendo do status do objeto.

Esta ação está selecionada por padrão.

Na seção **Proteção Contra Ameaças ao Correio**, é possível ativar ou desativar a Proteção Contra Ameaças ao Correio e selecionar a ação que o Kaspersky Endpoint Security executa ao detectar objetos maliciosos.

Ativar Proteção Contra Ameaças ao Correio

Esta caixa de seleção ativa/desativa a Proteção Contra Ameaças ao Correio.

Essa caixa de seleção está marcada por padrão.

Exclua objetos maliciosos automaticamente

Quando o Kaspersky Endpoint Security detecta um objeto infectado em uma mensagem de e-mail, ele exclui o objeto infectado e substitui o conteúdo dele pelo texto "The requested file infected with <nome do vírus> has been deleted".

Bloqueie objetos maliciosos automaticamente

Quando o Kaspersky Endpoint Security detecta um objeto infectado em uma mensagem de e-mail, ele substitui o assunto da mensagem por "Message is infected: <assunto original>", sendo <assunto original> o assunto da mensagem original. O assunto da mensagem de e-mail só é substituído para o protocolo POP3.

Na seção **Proteção Contra Ameaças à Rede**, é possível ativar ou desativar a Proteção Contra Ameaças à Rede.

Ativar Proteção Contra Ameaças à Rede

Esta caixa de seleção ativa/desativa a Proteção Contra Ameaças à Rede.

Essa caixa de seleção está marcada por padrão.

Ajustes

Clicar neste botão abre uma janela na qual você pode criar uma lista de computadores confiáveis ou exibir e editar a lista de computadores bloqueados.



Clicar neste botão impede que usuários sem privilégios de administrador modifiquem as configurações do aplicativo Kaspersky Endpoint Security.



Clicar nesse botão abre um prompt para credenciais de administrador. Após inserir as credenciais de administrador, as configurações do aplicativo se tornam editáveis.

A guia Aplicativos confiáveis

Na guia **Aplicativos confiáveis**, é possível criar uma lista de aplicativos que não deverão ser monitorados pelo aplicativo Kaspersky Endpoint Security.

Por padrão, a lista de objetos da Zona Confiável está vazia.

+

Clicar neste botão abre uma janela onde é possível inserir um caminho para um aplicativo, especificar seu requisito de assinatura de código e selecionar os tipos de atividade que não serão monitoradas pelo Kaspersky Endpoint Security.

–

Clicar nesse botão remove o aplicativo selecionado da Zona Confiável.

Editar

Clicar nesse botão abre uma janela na qual você pode editar os parâmetros do aplicativo confiável.

A janela Adicionar aplicativo confiável

Caminho

O caminho para um aplicativo cujas atividades de rede ou arquivo não serão monitoradas pelo Kaspersky Endpoint Security.

Observação: Links simbólicos não podem ser usados para especificar caminhos neste campo.

Selecionar

Clicar nesse botão abre uma janela na qual é possível selecionar um aplicativo cujas atividades de rede não serão monitoradas pelo Kaspersky Endpoint Security. Nesse caso, os valores dos campos **Caminho** e **Requisito de assinatura de código** são inseridos automaticamente.

Requisito de assinatura de código

Requisitos para a assinatura do código do aplicativo cuja atividade não será monitorada pelo Kaspersky Endpoint Security.

Este é um parâmetro opcional.

Na seção **Opções**, você pode selecionar o tipo de atividade que não deseja que seja monitorada pelo aplicativo Kaspersky Endpoint Security.

Não monitorar a atividade de arquivos

Esta caixa de seleção ativa/desativa o monitoramento das operações de um aplicativo com arquivos em um computador cliente.

Se esta caixa de seleção estiver marcada, o Kaspersky Endpoint Security não monitorará a atividade de arquivos do aplicativo.

Se esta caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security monitorará a atividade de arquivos do aplicativo.

Esta caixa de seleção está marcada por padrão.

Não monitorar a atividade de rede

Esta caixa de seleção ativa/desativa o monitoramento do tráfego de entrada e saída da Internet do aplicativo em um computador cliente.

Se a caixa de seleção estiver marcada, o Kaspersky Endpoint Security não monitorará a atividade de rede do aplicativo.

Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security monitorará a atividade de rede do aplicativo.

Esta caixa de seleção está marcada por padrão.

Cancelar

Clicar nesse botão fecha a janela sem salvar as mudanças.

OK

Clicar nesse botão salva os parâmetros do aplicativo confiável e fecha a janela.

A guia Arquivos e pastas confiáveis

Na guia **Arquivos e pastas**, é possível criar uma lista de arquivos e pastas que não deverão ser monitorados pelo aplicativo Kaspersky Endpoint Security.

Por padrão, a lista de objetos da Zona Confiável está vazia.

+
Clicar neste botão abre uma caixa de diálogo para seleção de um arquivo ou pasta.
–
Clicar neste botão remove o objeto selecionado da Zona Confiável.

A guia Endereços da Web confiáveis

Na guia **Endereços da Web**, é possível criar uma lista de endereços da Web que não deverão ser monitorados pelo aplicativo Kaspersky Endpoint Security.

Por padrão, a lista de objetos da Zona Confiável está vazia.

+
Clicar neste botão abre um campo para inserir o endereço da Web.
É possível usar os seguintes símbolos ao especificar o endereço do site:

- O símbolo de asterisco (`*`) substitui qualquer conjunto de caracteres, exceto os caracteres `\` e `/`.
- Dois asteriscos consecutivos (`**`) substituem qualquer conjunto de caracteres (incluindo um conjunto vazio), incluindo os caracteres `\` e `/`.
- O ponto de interrogação (`?`) substitui qualquer caractere único no nome do arquivo ou da pasta, exceto os caracteres `\` e `/`.

–

Clicar nesse botão remove o endereço da Web selecionado Zona Confiável.

A janela de Ajustes da Proteção Contra Ameaças ao Correio

Ignorar arquivos maiores que <valor> MB

Caso esta caixa de seleção esteja marcada, a Proteção Contra Ameaças ao Correio excluirá da verificação os arquivos comprimidos anexados nas mensagens de e-mail se o tamanho exceder o valor especificado.

Caso esta caixa de seleção esteja desmarcada, a Proteção Contra Ameaças ao Correio verificará os arquivos compactados de anexos de e-mail de qualquer tamanho.

O valor padrão é 8 MB.

Essa caixa de seleção está marcada por padrão.

Limitar o tempo para a verificação de arquivos compactados a <valor> s

Caso esta caixa de seleção esteja marcada, o tempo alocado para a verificação de arquivos comprimidos anexados a mensagens de e-mail será limitado ao período especificado.

Caso esta caixa de seleção esteja desmarcada, o tempo alocado para a verificação de arquivos comprimidos não será limitado.

O valor padrão é 5 segundos.

Essa caixa de seleção está marcada por padrão.

A janela “Configurações”

Na guia **Computadores confiáveis**, é possível criar uma lista de computadores confiáveis. O aplicativo Kaspersky Endpoint Security não bloqueará os endereços IP desses computadores automaticamente, mesmo se for detectada uma atividade de rede perigosa associada a eles.

A lista de computadores confiáveis está vazia por padrão.

+

Clicar nesse botão adiciona um campo para inserir o endereço IP de um computador confiável.

–

Clicar nesse botão remove o endereço IP selecionado da lista de computadores confiáveis.

Editar

Clicar nesse botão permite editar o endereço IP selecionado.

Na guia **Computadores bloqueados**, é possível ver e editar a lista de computadores bloqueados.

O aplicativo Kaspersky Endpoint Security bloqueará o computador com esse endereço IP durante uma hora após detectar atividade de rede perigosa proveniente dele.

Endereço IP

Essa coluna exibe o endereço IP do computador bloqueado.

Hora do incidente

Esta coluna exibe a data e hora em que a atividade de rede perigosa foi detectada no computador.

Desbloquear

Clicar nesse botão remove o endereço IP selecionado da lista de computadores bloqueados.

A guia Regras de pacote de rede

Nome da regra

Nome da regra de pacote de rede.

Na seção **Ação**, é possível selecionar a ação a ser executada pelo Kaspersky Endpoint Security ao detectar a atividade de rede.

Na seção **Protocolo**, é possível especificar o protocolo ao qual a regra de rede se aplica.

Na seção **Direção**, é possível especificar a direção da atividade de rede sendo monitorada.

Na seção **TTL**, é possível especificar a vida útil dos pacotes de rede sendo monitorados.

Na seção **Adaptadores de rede**, é possível especificar os adaptadores de rede ao qual a regra de rede se aplica.

Na seção **Endereço remoto**, é possível especificar os endereços de rede dos dispositivos remotos que podem enviar e receber pacotes de rede.

Na seção **Endereço local**, é possível especificar os endereços de rede locais dos dispositivos que podem enviar e receber pacotes de rede.

Registrar eventos

Essa caixa de seleção ativa/desativa o registro de eventos do Firewall.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security registra os eventos do Firewall no relatório.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não registra os eventos do Firewall no relatório.

Essa caixa de seleção vem desmarcada por padrão.

A janela Adaptador de rede

Nome do adaptador

O nome do adaptador de rede.

Tipo de interface

Nessa lista suspensa, é possível selecionar o tipo de interface do adaptador de rede.

Endereços IP

A lista de endereços IP.

Endereços MAC

A lista de endereços MAC.

A janela de Adaptadores de rede

Nome

Essa coluna contém o nome do adaptador de rede.

Tipo de interface

Essa coluna contém o tipo de interface do adaptador de rede.

Endereços IP

Essa coluna contém os endereços IP do adaptador de rede.

Endereços MAC

Essa coluna exibe os endereços MAC do adaptador de rede.

A janela de Endereços locais

Endereços locais

Essa coluna contém os endereços locais.

A janela de Endereços locais

Tipo

Essa lista suspensa permite que você especifique o tipo de entrada de IP local à qual você deseja que a regra de rede se aplique.

Endereço IP

Campo de entrada Endereço IP. Este campo só ficará disponível se você selecionar **Endereço IP** na lista suspensa **Tipo**.

Início do intervalo

Campo de entrada Início do intervalo de endereços IP. Este campo só ficará disponível se você selecionar **Intervalo de endereços IP** na lista suspensa **Tipo**.

Fim do intervalo

Campo de entrada Fim do intervalo de endereços IP. Este campo só ficará disponível se você selecionar **Intervalo de endereços IP** na lista suspensa **Tipo**.

A janela de Endereços remotos

Endereços remotos

Essa coluna contém os endereços remotos.

A janela de Endereço remoto

Tipo

Essa lista suspensa permite que você especifique o tipo de entrada de endereço remoto à qual você deseja que a regra de rede se aplique.

Endereço

Campo de entrada de Endereço IP ou nome DNS. Este campo só ficará disponível se você selecionar **Endereço IP ou nome DNS** na lista suspensa **Tipo**.

Início do intervalo

Campo de entrada Início do intervalo de endereços IP. Este campo só ficará disponível se você selecionar **Intervalo de endereços IP** na lista suspensa **Tipo**.

Fim do intervalo

Campo de entrada Fim do intervalo de endereços IP. Este campo só ficará disponível se você selecionar **Intervalo de endereços IP** na lista suspensa **Tipo**.

A janela Modelos

Modelos da regra de rede

Esta coluna contém modelos de regras de rede.

A guia Regras de pacote de rede

Nome

Nome da regra de rede.

Ação

Ação a ser executada pelo Firewall ao detectar o tipo de atividade de rede.

Endereço

Endereços de rede aos quais a regra de rede é aplicada.

A guia Redes disponíveis

Nome

Essa coluna contém o nome da rede.

Status de rede

Essa coluna contém o status da rede.

Endereço IP

Essa coluna contém os endereços IP da rede.

A janela Rede disponível

Nome da rede

O nome da rede.

Status de rede

A lista suspensa de status da rede.

Endereço IP

O endereço IP da rede.

A janela Endereço MAC

Tipo

Essa lista suspensa permite que você especifique o tipo de entrada de endereço MAC à qual você deseja que a regra de rede se aplique.

Endereço MAC

Campo de entrada Endereço MAC. Este campo só ficará disponível se você selecionar **Endereço MAC** na lista suspensa **Tipo**.

Máscara

Campo de entrada máscara do endereço MAC. Este campo só ficará disponível se você selecionar **Máscara do endereço MAC** na lista suspensa **Tipo**.

Início do intervalo

Campo de entrada Início do intervalo de endereços MAC. Este campo só ficará disponível se você selecionar **Intervalo de endereços MAC** na lista suspensa **Tipo**.

Fim do intervalo

Campo de entrada Fim do intervalo de endereços MAC. Este campo só ficará disponível se você selecionar **Intervalo de endereços MAC** na lista suspensa **Tipo**.

A guia Avançado

Na seção **KSN**, é possível ler os termos da Declaração da Kaspersky Security Network e optar por participar ou não da Kaspersky Security Network.

Mostrar a Declaração da KSN

Clicar neste botão abre uma janela que exibe o texto da Declaração da Kaspersky Security Network.

O Kaspersky Endpoint Security pode usar a infraestrutura da KSN Global ou Privada. Se você participa na Kaspersky Security Network, o Kaspersky Endpoint Security usa informações sobre a reputação de arquivos, recursos da Web e aplicativos recebidos da Kaspersky Security Network e fornece os dados necessários para o funcionamento dos serviços de detecção para a Kaspersky Security Network.

Participar da Kaspersky Security Network

Essa caixa de seleção ativa/desativa a participação na Kaspersky Security Network.

Participar da Kaspersky Private Security Network

Esta caixa de seleção ativa/desativa a participação na Kaspersky Private Security Network. Para obter mais informações sobre a participação na Kaspersky Private Security Network, entre em contato com o administrador do sistema da organização.

Ativar modo KSN estendido

Esta caixa de seleção ativa/desativa o fornecimento de dados adicionais para a Kaspersky Security Network. Os dados são usados para melhorar a proteção de seu computador e a usabilidade do Kaspersky Endpoint Security. É possível encontrar a lista de dados na Declaração da Kaspersky Security Network e na ajuda do Kaspersky Endpoint Security.

Esta caixa de seleção é marcada automaticamente se a caixa de seleção **Participar da Kaspersky Security Network** estiver marcada.

Ativar modo na nuvem

O modo na nuvem refere-se ao modo operacional do aplicativo no qual o Kaspersky Endpoint Security usa uma versão leve de bancos de dados antimalware. Esse modo está disponível apenas se a participação na Kaspersky Security Network estiver ativada. A versão leve dos bancos de dados antimalware permite o uso de cerca de metade da memória RAM do computador que seria usada com os bancos de dados usuais. Se você não participar da Kaspersky Security Network ou se o modo na nuvem estiver desativado, o Kaspersky Endpoint Security baixará a versão completa dos bancos de dados antimalware dos servidores da Kaspersky.

Se o botão de alternância estiver ativado, o Kaspersky Endpoint Security usará a versão leve dos bancos de dados antimalware, o que reduz a carga nos recursos do sistema operacional.

> **Nota:** o Kaspersky Endpoint Security baixará a versão leve dos bancos de dados antimalware durante a próxima atualização após a caixa de seleção ser marcada.

Se o botão de alternância estiver desativado, o Kaspersky Endpoint Security usará a versão completa dos bancos de dados antimalware.

> **Nota:** o Kaspersky Endpoint Security baixará a versão completa dos bancos de dados antimalware durante a próxima atualização após a caixa de seleção ser desmarcada.

Na seção **Detecção de Comportamento**, é possível ativar/desativar o componente Detecção de Comportamento e selecionar uma ação a ser executada quando a atividade de malware for detectada.

Ativar Detecção de Comportamento

Essa caixa de seleção ativa/desativa o componente Detecção de Comportamento, que recebe informações sobre as ações dos aplicativos no computador para fornecê-las a outros componentes de proteção para melhorar o desempenho.

Bloquear atividade de malwares

Caso essa opção seja selecionada, o Kaspersky Endpoint Security encerrará o aplicativo ao detectar atividade maliciosa.

Excluir objetos perigosos detectados

Caso essa opção seja selecionada, o Kaspersky Endpoint Security excluirá o arquivo executável de um aplicativo malicioso e criará uma cópia backup do arquivo no Backup quando uma atividade maliciosa for detectada.

Perguntar o que fazer

Caso esta opção esteja selecionada, quando a atividade de malware for detectada, o aplicativo Kaspersky Endpoint Security exibirá uma janela de notificação com as informações sobre o objeto malicioso e solicitará que o usuário escolha a ação a ser executada pelo aplicativo Kaspersky Endpoint Security. As ações disponíveis podem variar dependendo do status do objeto.



Clicar neste botão impede que usuários sem privilégios de administrador modifiquem as configurações do aplicativo Kaspersky Endpoint Security.



Clicar nesse botão abre um prompt para credenciais de administrador. Após inserir as credenciais de administrador, as configurações do aplicativo se tornam editáveis.

A guia Verificação

Lista das tarefas de verificação de malware

Contém as seguintes tarefas pré-definidas de verificação de malware:

- **Verificação completa**. Uma verificação de malware da memória, objetos de inicialização e todos os discos internos do computador.
- **Verificação rápida**. Uma verificação de malware apenas nas áreas mais importantes do computador: memória, objetos de inicialização e pastas do sistema.
- **Verificação personalizada**. Uma verificação de malware de um objeto especificado (arquivo, pasta, disco interno ou removível).
- **Verificação dos discos externos**. Uma verificação de malware nos discos externos realizada quando um disco externo é conectado ao computador.

Nota: o Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.

Na seção **Escopo da verificação**, é possível visualizar e editar o escopo da verificação da tarefa Verificação Rápida.

Editar

Clicar nesse botão abre uma janela na qual você pode ver e editar o escopo de verificação.

Este botão aparece somente quando a tarefa de Verificação Rápida for selecionada na lista.

Na seção **Ação**, é possível selecionar a ação que o Kaspersky Endpoint Security executará ao detectar um arquivo infectado e agendar uma tarefa.

Desinfectar ou excluir objetos maliciosos automaticamente

O Kaspersky Endpoint Security bloqueia o acesso ao arquivo infectado e tenta desinfectá-lo sem solicitar a confirmação do usuário. Antes de executar a desinfecção, o Kaspersky Endpoint Security salva uma cópia de backup do arquivo no Backup. Se a desinfecção for bem-sucedida, o Kaspersky Endpoint Security salvará o arquivo em sua localização original com o nome original do arquivo. Se ocorrer falha na desinfecção, o Kaspersky Endpoint Security manterá o arquivo infectado bloqueado e em sua localização original. As informações sobre a detecção do objeto infectado são registradas no relatório **Objetos processados**.

Perguntar após a verificação

O Kaspersky Endpoint Security adia o processamento dos arquivos infectados que foram detectados até o fim da verificação. Quando a verificação for concluída, o Kaspersky Endpoint Security exibe janelas de notificações que informam sobre cada objeto infectado detectado e oferece opções de ações complementares. As ações disponíveis podem variar dependendo do status do objeto.

Esta ação está selecionada por padrão.

Na seção **Quando um disco externo for conectado** da guia **Verificação dos discos externos**, você pode selecionar a ação que o Kaspersky Endpoint Security executa quando um disco externo é conectado.

Verificação

Se essa opção for selecionada, o Kaspersky Endpoint Security iniciará uma tarefa de verificação de malware para o disco externo conectado.

Esta opção está marcada por padrão.

Nenhuma ação

Se essa opção estiver selecionada, o Kaspersky Endpoint Security não verificará o disco externo conectado.

Na seção **Otimização**, é possível configurar se o aplicativo da Kaspersky Endpoint Security verificará o volume do sistema somente leitura ao executar uma tarefa de Verificação Rápida ou Verificação Completa.

Ignorar a verificação de volumes de sistema somente leitura

Esta caixa de seleção ativa/desativa a verificação do volume do sistema somente leitura pelo Kaspersky Endpoint Security.

Esta caixa de seleção é marcada por padrão para uma tarefa de Verificação Rápida e desmarcada por padrão para uma tarefa de Verificação Completa.

Importante: a otimização pode estar desativada por motivos de segurança.

Uso de CPU

Clicar neste botão abre uma caixa de diálogo onde é possível ativar ou desativar a limitação do uso da CPU do dispositivo protegido pelo aplicativo para tarefas de verificação. Se a opção **Limitar utilização de CPU por verificações a** estiver selecionada, é possível especificar o uso máximo da CPU permitido no campo correspondente.

Observação: O limite é acumulativo de todos os núcleos da CPU. O uso da CPU exibido no Monitor de Atividade é a soma do uso de cada núcleo da CPU e pode ficar acima de 100%.

A ativação dessa opção pode afetar negativamente o desempenho do Kaspersky Endpoint Security.

Essa opção é desativada por padrão.

Agendamento

Clicar neste botão abre uma caixa de diálogo onde você pode agendar tarefas de Verificação Rápida ou Verificação Completa.



Clicar neste botão impede que usuários sem privilégios de administrador modifiquem as configurações do aplicativo Kaspersky Endpoint Security.



Clicar nesse botão abre um prompt para credenciais de administrador. Após inserir as credenciais de administrador, as configurações do aplicativo se tornam editáveis.

A guia Ameaças

Na seção **Objetos a detectar**, é possível configurar a lista de objetos a serem detectados.

Vírus, worms, trojans, ferramentas maliciosas, adwares e discadores automáticos

Esta categoria inclui os seguintes tipos de programas:

- Todos os tipos de malware.
- Aplicativos que mostram anúncios (como banners) no seu computador ou que substituem os resultados de pesquisa no navegador por sites de publicidade.
- Aplicativos que secretamente estabelecem conexões telefônicas através do modem de um computador.

O Kaspersky Endpoint Security sempre controla programas deste tipo.

A caixa de seleção está sempre marcada e não pode ser desmarcada.

Softwares legítimos que podem ser usados por intrusos para danificar seu computador ou dados pessoais

Essa caixa de seleção ativa/desativa o controle de aplicativos legítimos que podem ser explorados por um intruso para danificar o computador ou os dados do usuário, como aplicativos de administração remota.

Essa caixa de seleção vem desmarcada por padrão.

Na seção **Backup**, é possível especificar por quanto tempo os objetos podem ser armazenados no Backup.

Excluir backups de objetos após <valor> dias

Esta caixa de seleção ativa/desativa a remoção de objetos do Backup após o período especificado.

Se a caixa de seleção estiver marcada, o aplicativo excluirá os objetos do Backup após o período especificado no campo numérico ao lado da caixa de seleção. Se a caixa de seleção estiver desmarcada, os objetos serão armazenados no Backup por tempo indefinido.

Por padrão, essa caixa de seleção está marcada e os objetos são armazenados no Backup durante 30 dias.

Na seção **Exclusões**, é possível criar uma lista de arquivos, pastas, aplicativos e sites confiáveis e que não deseja que sejam verificados em busca de malware.

Zona Confiável

Clicar nesse botão abre uma janela onde você pode editar a Zona Confiável criando uma lista de objetos nos quais você confia e não deseja verificar se há malware.

> **Nota:** Quando um administrador configura a política para proibir a edição da zona confiável, os usuários não podem acessar os ajustes dela.



Clicar neste botão impede que usuários sem privilégios de administrador modifiquem as configurações do aplicativo Kaspersky Endpoint Security.



Clicar nesse botão abre um prompt para credenciais de administrador. Após inserir as credenciais de administrador, as configurações do aplicativo se tornam editáveis.

A guia Atualização

Na seção **Bancos de dados**, é possível configurar o modo de atualização de bancos de dados do Kaspersky Endpoint Security.

Baixar atualizações automaticamente

Essa caixa de seleção ativa/desativa as atualizações automáticas dos bancos de dados do aplicativo.

Essa caixa de seleção está marcada por padrão.

Na seção **Proxy**, é possível configurar o uso de um servidor proxy para atualizar o Kaspersky Endpoint Security.

Usar servidor proxy

Esta caixa de seleção ativa/desativa o uso de um servidor proxy para conectar à Internet ao atualizar bancos de dados de antimalware e módulos do aplicativo.

Essa caixa de seleção está marcada por padrão.

Ajustes

Clicar nesse botão abre uma janela onde é possível definir as configurações de conexão do servidor proxy.

Na seção **Reversão**, é possível reverter para a versão anterior dos bancos de dados do aplicativo. Pode ser necessário reverter as atualizações quando a nova versão dos bancos de dados do aplicativo contiver uma assinatura incorreta que faça com que o Kaspersky Endpoint Security bloqueie um aplicativo seguro.

Reverter atualização

Clicar nesse botão executa a reversão dos bancos de dados do aplicativo.



Clicar neste botão impede que usuários sem privilégios de administrador modifiquem as configurações do aplicativo Kaspersky Endpoint Security.



Clicar nesse botão abre um prompt para credenciais de administrador. Após inserir as credenciais de administrador, as configurações do aplicativo se tornam editáveis.

A janela Configurações do servidor proxy

Usar os ajustes do servidor proxy do sistema

O Kaspersky Endpoint Security usa as configurações do servidor proxy especificadas no Ajuste do Sistema do seu Mac.

Esta ação está selecionada por padrão.

Usar os ajustes do servidor proxy especificado

O Kaspersky Endpoint Security usa as configurações do servidor proxy especificadas nesta janela.

Endereço

Campo para inserir o endereço IP ou o nome de domínio de um servidor proxy.

Este campo ficará disponível se a opção **Usar os ajustes do servidor proxy especificado** for marcada.

Porta

Campo de entrada para o número da porta do servidor proxy usada para atualizar o Kaspersky Endpoint Security.

Este campo ficará disponível se a opção **Usar os ajustes do servidor proxy especificado** for marcada.

O valor padrão é 80.

Usar autenticação

Autenticação é o processo de verificação do nome de usuário e senha ao se conectar a um servidor proxy.

Essa caixa de seleção ativa/desativa a autenticação ao conectar-se a um servidor proxy.

Essa caixa de seleção vem desmarcada por padrão.

Nome do usuário

Campo para inserir o nome de usuário para autenticação ao conectar-se ao servidor proxy.

O campo estará disponível se a caixa de seleção **Usar autenticação** estiver marcada.

Senha

Campo para inserir a senha para autenticação ao conectar-se ao servidor proxy.

O campo estará disponível se a caixa de seleção **Usar autenticação** estiver marcada.

Se você não especificou o nome de usuário e a senha, ou se o nome de usuário e a senha especificados foram rejeitados pelo servidor proxy, uma janela é aberta na qual será necessário inserir o nome de usuário e a senha para autenticação no servidor proxy. Se a autenticação for bem-sucedida e a caixa de seleção **Lembrar senha** estiver marcada na janela de solicitação, o nome de usuário e a senha especificados serão aplicados em todos os casos no futuro. Se a caixa de seleção **Lembrar senha** estiver desmarcada na janela de entrada de nome de usuário e senha, o nome de usuário e a senha serão solicitados novamente na próxima conexão com o servidor proxy.

Ignorar servidor proxy para endereços locais

Essa caixa de seleção ativa/desativa o uso de um servidor proxy ao atualizar o aplicativo a partir de uma pasta local ou de rede.

Essa caixa de seleção está marcada por padrão.

A caixa de diálogo Autenticação do servidor proxy obrigatória

Nome do usuário

Campo para inserir o nome do usuário para conectar ao servidor proxy.

Senha

Campo para inserir a senha.

Lembrar senha

Esta caixa de seleção habilita/desabilita o uso do nome de usuário e senha especificado para autenticação no servidor proxy no futuro.

Essa caixa de seleção vem desmarcada por padrão.

A guia Interface

Na seção **Notificações**, é possível definir as notificações que o Kaspersky Endpoint Security exibe para informá-lo sobre vários eventos.

Ativar notificações

Essa caixa de seleção ativa/desativa as notificações sobre eventos do aplicativo.

Essa caixa de seleção está marcada por padrão.

Ativar sons de alerta ao detectar malware

Essa caixa de seleção ativa/desativa os alertas sonoros quando o Kaspersky Endpoint Security detecta um objeto malicioso.

Essa caixa de seleção está marcada por padrão.

Na seção **Ícone do aplicativo**, é possível configurar o ícone do aplicativo a ser exibido na barra de menus.

Exibir na barra de menus

Essa caixa de seleção ativa/desativa a exibição do ícone do aplicativo na barra de menus.

Na seção **Relatórios**, é possível ativar/desativar o registro de eventos não críticos nos relatórios do Kaspersky Endpoint Security.

Registrar eventos não críticos

Essa caixa de seleção ativa/desativa o registro de eventos informativos nos relatórios. Em geral, esses eventos não são importantes para a segurança do computador.

Na seção **Rastros**, é possível ativar ou desativar o rastreamento.

O rastreamento é uma maneira de registrar informações detalhadas sobre a atividade do aplicativo. Os especialistas do Suporte Técnico da Kaspersky usam arquivos de rastreamento para solucionar problemas. Você pode ativar o registo de eventos do aplicativo para criar arquivos de rastreamento e enviá-los ao Suporte Técnico, caso solicitado. Por padrão, o registo de eventos do aplicativo fica desativado.

Importante: ative o rastreamento somente quando um especialista do Suporte Técnico pedir que você faça isso.

Ativar rastreamento

Esta caixa de seleção ativa/desativa a criação de arquivos de rastreamento.

Essa caixa de seleção vem desmarcada por padrão.

Na seção **Proteção por senha**, você pode ativar a proteção por senha de ações indesejadas em seu computador.

Ativar a proteção por senha

Esta caixa de seleção ativa/desativa a proteção por senha de ações indesejadas.

Essa caixa de seleção vem desmarcada por padrão.

Marcar esta caixa de seleção abre uma janela onde você pode definir e configurar a senha de administrador.

Ajustes

Clicar neste botão abre uma janela na qual você pode editar os parâmetros da senha de administrador.



Clicar neste botão impede que usuários sem privilégios de administrador modifiquem as configurações do aplicativo Kaspersky Endpoint Security.



Clicar nesse botão abre um prompt para credenciais de administrador. Após inserir as credenciais de administrador, as configurações do aplicativo se tornam editáveis.

A janela Configurar senha de administrador

Senha

Campo para inserir uma senha para limitar ações indesejadas no dispositivo.

Confirmar senha

Campo para confirmação de senha inserindo-a uma segunda vez.

Opções

A lista de ações que podem ser protegidas pela senha. Marque as caixas de seleção necessárias para proteger as ações correspondentes no dispositivo. Você deve marcar pelo menos uma caixa de seleção.

Cancelar

Clicar nesse botão fecha a janela sem salvar as mudanças.

OK

Clicar nesse botão salva os ajustes de senha do administrador e fecha a janela. Depois que as alterações forem salvas, você será solicitado a inserir a senha ao tentar executar uma ação indesejada no dispositivo.

O relatório de Eventos do sistema

O painel direito da janela contém um relatório sobre o funcionamento do Kaspersky Endpoint Security.

Hora

Essa coluna exibe a data e a hora do evento.

Evento

Essa coluna exibe o status do evento.

Nome do Programa

Esta coluna exibe o nome do programa no qual o evento ocorreu.

Usuário

Essa coluna exibe o nome do usuário que iniciou o evento.

Tipo de usuário

Esta coluna exibe o nome do usuário que iniciou o evento.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

Relatório Objetos processados

O painel à direita da janela contém a lista de todos os objetos infectados e objetos perigosos no tráfego da Web detectados pelo aplicativo Kaspersky Endpoint Security.

Hora

Essa coluna exibe a hora em que o objeto foi detectado.

Objeto

Essa coluna exibe o caminho para o local onde o objeto foi detectado ou o endereço da Web do objeto.

Status

Essa coluna exibe a ação que o aplicativo executou após detectar o objeto.

Detectado(a)

Essa coluna exibe o tipo do objeto detectado de acordo com a classificação da Virus Encyclopedia da Kaspersky.

Nome

Essa coluna exibe o nome do objeto detectado de acordo com a classificação da Virus Encyclopedia da Kaspersky.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

O relatório de Atualização do banco de dados

O painel da direita da janela contém relatórios sobre as tarefas de atualização executadas pelo aplicativo.

Iniciado

Essa coluna exibe a data e a hora de início de cada tarefa de atualização. Caso a lista de operações seja expandida, esta coluna também listará as operações executadas durante a atualização do aplicativo e a hora nas quais foram executadas.

Status

Esta coluna exibe o status da tarefa de atualização.

Tamanho

Essa coluna exibe o tamanho dos arquivos de atualização baixados.

Velocidade média

Esta coluna exibe a velocidade do download do arquivo de atualização.

Hora do fim

Esta coluna exibe a hora de finalização da tarefa de atualização.

Clicar nesse botão expande a lista de operações incluídas na tarefa de atualização.

Clicar nesse botão contrai a lista de operações incluídas na tarefa de atualização.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

Relatório de verificação

O painel da direita da janela contém relatórios sobre as tarefas de verificação executadas pelo Kaspersky Endpoint Security.

Tarefa

Esta coluna exibe o nome da tarefa de verificação.

Status

Essa coluna exibe o status de uma tarefa de verificação de vírus ou o status dos objetos verificados.

Data

Essa coluna exibe a data e a hora de uma tarefa de verificação.

Iniciador

Essa coluna exibe o usuário, aplicativo ou processo que iniciou uma tarefa de verificação.

Clicar neste botão expande a lista de objetos verificados.

Clicar neste botão exibe a lista de objetos verificados.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

Relatório de Proteção Contra Ameaças ao Arquivo

O painel direito da janela contém um relatório sobre o funcionamento da Proteção Contra Ameaças ao Arquivo.

Data

Esta coluna exibe data e hora em que o aplicativo acessou um objeto verificado.

Caminho

Esta coluna exibe o caminho à localização original de um objeto verificado.

Status

Esta coluna exibe o status de um objeto verificado.

Nome do Programa

Esta coluna exibe o aplicativo que acessou um objeto verificado.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

O relatório de Proteção Contra Ameaças da Web

O painel direito da janela contém um relatório sobre o funcionamento da Proteção Contra Ameaças da Web.

Data

Esta coluna exibe data e hora em que os objetos de tráfego na Web foram detectados.

URL

Esta coluna exibe os objetos de tráfego da Web que foram detectados pela Proteção Contra Ameaças da Web. A coluna especifica o endereço da Web em que cada objeto foi detectado no tráfego da Web.

Status

Esta coluna exibe o status de objetos de tráfego da Web que foram detectados.

Nome do programa

Esta coluna exibe o programa que acessou os objetos de tráfego da Web detectados.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

O relatório da Proteção Contra Ameaças ao Correio

O painel direito da janela contém um relatório sobre o funcionamento da Proteção Contra Ameaças ao Correio.

Data

Essa coluna exibe a data e hora em que um objeto infectado foi detectado numa mensagem de e-mail.

Caminho

Essa coluna exibe informações sobre a mensagem de e-mail em que o objeto infectado foi detectado.

Status

Essa coluna exibe a ação executada pelo Kaspersky Endpoint Security após detectar um objeto infectado.

Nome do programa

Essa coluna exibe o nome do cliente de e-mail.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

O relatório de Proteção Contra Ameaças à Rede

O painel direito da janela contém um relatório sobre o funcionamento da Proteção Contra Ameaças à Rede.

Data

Esta coluna exibe a data e hora em que a atividade de rede perigosa foi detectada no computador.

Endereço IP

Esta coluna exibe o endereço IP do computador cuja atividade de rede perigosa foi detectada pelo Kaspersky Endpoint Cloud.

Status

Esta coluna exibe a ação executada pelo Kaspersky Endpoint Security após detectar atividade de rede perigosa.

Tipo de ataque

Esta coluna exibe o tipo de ataque à rede detectado.

Porta local

Esta coluna exibe o número da porta local através da qual foi detectada uma tentativa de intrusão.

Protocolo

Esta coluna exibe o tipo de protocolo usado para executar o ataque.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

O relatório do Endpoint Detection and Response

O painel direito da janela contém um relatório sobre o funcionamento do componente Endpoint Detection and Response.

Data

Essa coluna exibe a data e a hora dos eventos.

Evento

Essa coluna exibe o status dos eventos.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

O relatório do Firewall

O painel direito da janela contém um relatório sobre o funcionamento do Firewall.

Data

Essa coluna exibe a data e a hora dos eventos.

Evento

Essa coluna exibe o status dos eventos.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

O relatório da Prevenção de Exploits

O painel direito da janela contém um relatório sobre o funcionamento da Prevenção de Exploits.

Data

Essa coluna exibe a data e a hora dos eventos.

Evento

Essa coluna exibe o status dos eventos.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

O relatório do Controle de Dispositivos

O painel direito da janela contém um relatório sobre o funcionamento do Controle de dispositivos.

Data

Essa coluna exibe a data e a hora dos eventos.

Evento

Essa coluna exibe o status dos eventos.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

O relatório do Inspetor do Sistema

O painel direito da janela contém um relatório sobre o funcionamento do componente Inspetor do Sistema.

Data

Essa coluna exibe a data e a hora dos eventos.

Evento

Essa coluna exibe o status dos eventos.



Clicar nesse botão abre uma janela que permite salvar o relatório como um arquivo TXT.

A janela Tipo de instalação

Na seção **Pacotes para instalar**, é possível selecionar os componentes do aplicativo que serão instalados em um computador cliente.

Verificação

Essa caixa de seleção adiciona o Componente de verificação ao pacote de instalação do Kaspersky Endpoint Security.

A caixa de seleção está marcada por padrão e não pode ser desmarcada.

Proteção Contra Ameaças ao Arquivo

Esta caixa de seleção ativa/desativa a adição do componente de Proteção Contra Ameaças ao Arquivo ao pacote de instalação do Kaspersky Endpoint Security.

Se essa caixa de seleção estiver marcada, o componente da Proteção Contra Ameaças ao Arquivo será incluído no pacote de instalação do Kaspersky Endpoint Security.

Se essa caixa de seleção estiver desmarcada, o componente da Proteção Contra Ameaças ao Arquivo não será incluído no pacote de instalação do Kaspersky Endpoint Security.

Esta caixa de seleção está marcada por padrão.

Proteção Contra Ameaças da Web

Essa caixa de seleção ativa/desativa a adição do componente de Proteção Contra Ameaças da Web ao pacote de instalação do Kaspersky Endpoint Security.

Se essa caixa de seleção estiver marcada, o componente da Proteção Contra Ameaças da Web será incluído no pacote de instalação do Kaspersky Endpoint Security.

Se essa caixa de seleção estiver desmarcada, o componente da Proteção Contra Ameaças da Web não será incluído no pacote de instalação do Kaspersky Endpoint Security.

Esta caixa de seleção está marcada por padrão.

Proteção Contra Ameaças à Rede

Esta caixa de seleção ativa/desativa a adição do componente de Proteção Contra Ameaças à Rede ao pacote de instalação do Kaspersky Endpoint Security.

Se essa caixa de seleção estiver marcada, o componente da Proteção Contra Ameaças à Rede será incluído no pacote de instalação do Kaspersky Endpoint Security.

Se essa caixa de seleção estiver desmarcada, o componente da Proteção Contra Ameaças à Rede não será incluído no pacote de instalação do Kaspersky Endpoint Security.

Esta caixa de seleção está marcada por padrão.

Conector do Agente de Rede

Essa caixa de seleção adiciona o componente do Conector do Agente de Rede ao pacote de instalação do Kaspersky Endpoint Security.

A caixa de seleção está marcada por padrão e não pode ser desmarcada.

A janela “Ajustes de proteção por senha”

Senha

Campo para inserir uma senha para limitar ações indesejadas nos dispositivos dos usuários.

Clique em **Exibir** para visualizar os símbolos inseridos.

Confirmar senha

Campo para confirmação de senha inserindo-a uma segunda vez.

Clique em **Exibir** para visualizar os símbolos inseridos.

Requer senha para

A lista de ações que podem ser protegidas pela senha. Marque as caixas de seleção necessárias para proteger as ações correspondentes no dispositivo do usuário.

A caixa de diálogo “Conceder acesso”

Obter chave de recuperação

Clicar nesse botão gera uma chave de recuperação necessária para acessar um disco criptografado em um computador cliente.

A seção Proteção Avançada Contra Ameaças

Na seção **Configurações da KSN**, é possível configurar o uso da Kaspersky Security Network.

Kaspersky Security Network

O botão do **Kaspersky Security Network** ativa/desativa a participação na Kaspersky Security Network.

Se o botão do **Kaspersky Security Network** estiver ativado, os computadores clientes aos quais a política é aplicada participarão da Kaspersky Security Network.

Se o botão do **Kaspersky Security Network** estiver desativado, os computadores clientes aos quais a política é aplicada não participarão da Kaspersky Security Network.

Por padrão, esse botão está desativado.

Modo KSN estendido

O botão do **Modo KSN estendido** ativa/desativa o envio de dados adicionais do computador remoto para a Kaspersky. Os dados são usados para melhorar a proteção dos computadores cliente e a usabilidade do Kaspersky Endpoint Security.

Se o **modo KSN estendido** estiver ligado, os computadores cliente regidos pela política fornecerão tanto os dados exigidos para o funcionamento dos serviços de detecção quanto os dados adicionais à Kaspersky Security Network.

Caso o **Modo KSN estendido** esteja desligado, os computadores cliente regidos pela política fornecerão somente os dados exigidos para o funcionamento dos serviços de detecção. Nenhum dado adicional será fornecido à Kaspersky Security Network.

Por padrão, o botão do **Modo KSN estendido** está desativado.

O botão é ativado automaticamente ao ativar o botão do **Kaspersky Security Network**, mas é possível desativá-lo.

Dados fornecidos à Kaspersky ao usar a Kaspersky Security Network na infraestrutura da KSN Global

Se o botão da **Kaspersky Security Network** estiver ativado e o botão do **Modo Estendido da KSN** estiver desativado, o Kaspersky Endpoint Security em execução nos computadores cliente fornece à Kaspersky os seguintes dados:

- Informações sobre a licença usada: o tipo e o período de validade da licença, número de dias até a expiração da licença, identificador do parceiro de quem a licença foi adquirida, identificador do Centro de Ativação Regional, soma de verificação do código de ativação, hash do corpo do tíquete calculado usando o algoritmo SHA1, data e hora da criação do tíquete de licença, identificador de informações da licença, identificador do tíquete de licença, identificador da sequência do tíquete de licença, identificador exclusivo do computador do usuário, data a partir da qual o tíquete de licença começa a valer, data de expiração da validade do tíquete de licença, estado atual do tíquete de licença, versão do cabeçalho do tíquete, versão da licença, identificador do certificado de assinatura do cabeçalho do tíquete, soma de verificação do arquivo de chave, número de série do assinante do cabeçalho do tíquete, token de autenticação.

- Versão completa do software instalado;
  tipo do Software instalado;
  ID de atualização do Software; ID do serviço de reputação; ID do tipo de protocolo; ID de um centro de ativação regional; versão da lista de decisões revogadas do serviço de Software; ID do registro acionado nos bancos de dados de antivírus do Software; carimbo de data e hora do registro acionado nos bancos de dados de antivírus do Software; tipo do registro acionado nos bancos de dados de antivírus do Software; ID exclusiva da instância da instalação do aplicativo no computador; data de ativação da licença; data de expiração da licença; identificador da licença; status da licença usada pelo Software; tipo de soma de verificação do objeto que está

sendo processado; nome do malware detectado ou do software legítimo que pode ser usado para causar danos ao dispositivo ou aos dados do usuário; soma de verificação do objeto que está sendo processado; soma de verificação do código de ativação do Software; versão completa do Software; ID exclusivo do dispositivo; ID do Software; soma de verificação do arquivo da chave do Software; ID do modelo de informações usado para fornecer a licença do Software; identificador do certificado usado para assinar o cabeçalho do tíquete de licença do Software; data e hora de criação do tíquete de licença do Software; a soma de verificação do tíquete de licença do Software; a versão do tíquete de licença do Software; a versão do código de ativação do Software; formato dos dados na solicitação para a infraestrutura do Titular dos Direitos; ID do tíquete de licença atual; o ID de componente do Software; o resultado da ação do Software; código de erro; endereço acessado do serviço Web (URL, IP); número da porta; endereço web da origem da solicitação de serviço da web (referenciador); chave pública do certificado; impressão digital do certificado digital do objeto verificado e algoritmo de hash.

Se os botões da **Kaspersky Security Network** e do **Modo Estendido da KSN** estiverem ativados, o Kaspersky Endpoint Security em execução nos computadores cliente fornece à Kaspersky os seguintes dados:

- Informações sobre a versão do sistema operacional (SO) e os service packs instalados no computador, a versão e as somas de verificação (MD5, SHA2-256, SHA1) do arquivo de kernel do SO, parâmetros do modo de execução do SO; versão do SO, número da compilação do SO, número da atualização do SO, edição do SO, informações estendidas sobre a edição do SO; versão do Service Pack do SO; data e hora da inicialização do SO; tempo de atraso do processamento do evento sobre a ação do SO no subsistema de análise comportamental; número de eventos da ação atrasada do SO do tipo atual; tempo de atraso de processamento do evento sobre a ação do SO no subsistema de defesa proativo; número de eventos processadas de ação do SO; número de eventos da ação processada síncrona do SO; atraso total de todos os eventos da ação do SO do tipo atual; tempo de atraso de processamento do evento sobre a ação do SO no subsistema de armazenamento de eventos persistentes; atraso total de todos os eventos da ação do SO; número de eventos da ação em espera síncrona do SO; data e hora do evento recebido de uma ação no SO.

- Informações sobre a última reinicialização do SO com falha: número de reinicializações com falha.

- Informações sobre o aplicativo instalado do Titular dos direitos e o status da proteção antivírus: ID de instalação do Software (PCID); Versão do registro do banco de dados do software; identificados exclusivo da instância da instalação do aplicativo no computador, tipo do aplicativo, ID do tipo do aplicativo, a versão completa do aplicativo instalado, a versão do identificador das configurações do aplicativo, o identificador do tipo de computador, o identificador exclusivo do computador em que o aplicativo está instalado, o identificador exclusivo do Usuário nos serviços do Titular de Direitos, idioma local e estado da operação, versão dos componentes do Software instalado e seus estados de operação, versão do protocolo usado para conectar com os serviços do Titular de Direitos; versão completa do software instalado; tipo do Software instalado; ID de atualização do Software; ID do serviço de reputação; ID do tipo de protocolo; ID de um centro de ativação regional; versão da lista de decisões revogadas do serviço de Software; ID do registro acionado nos bancos de dados de antivírus do Software; carimbo de data e hora do registro acionado nos bancos de dados de antivírus do Software; tipo do registro acionado nos bancos de dados de antivírus do Software; ID exclusiva da instância da instalação do aplicativo no computador; data de ativação da licença; data de expiração da licença; identificador da licença; status da licença usada pelo Software; tipo de soma de verificação do objeto que está sendo processado; nome do malware detectado ou do software legítimo que pode ser usado para causar danos ao dispositivo ou aos dados do usuário; soma de verificação do objeto que está sendo processado; soma de verificação do código de ativação do Software; versão completa do Software; ID do Software; soma de verificação do arquivo da chave do Software; ID do modelo de informações usado para fornecer a licença do Software; identificador do certificado usado para assinar o cabeçalho do tíquete de licença do Software; data e hora de criação do tíquete de licença do Software; a soma de verificação do tíquete de licença do Software; a versão do tíquete de licença do Software; a versão do código de ativação do Software; formato dos dados na solicitação para a infraestrutura do Titular dos Direitos; ID do tíquete de licença atual; o ID de componente do Software; o resultado da ação do Software; código de erro; endereço acessado do serviço Web (URL, IP); número da porta; endereço web da origem da solicitação de serviço da web (referenciador); número de ciclos atualização-aplicação para bases de dados antivírus; data e hora em que as bases de dados de antivírus foram atualizadas e aplicadas pela última vez; data e hora do lançamento nos bancos de dados do Software; versão do componente do Software; ID de atualização do Software; tipo do Software instalado; data e hora da inicialização do Inspetor do Sistema; data e hora da instalação do Software; probabilidade de enviar estatísticas pelo Inspetor do Sistema; código do evento que demorou mais tempo do que o tempo padrão a processar pelo Inspetor do Sistema; tempo de processamento da base de dados do evento que demorou mais tempo do que o tempo padrão a processar pelo Inspetor do Sistema; tempo máximo permitido para processamento de um evento pelo Inspetor do Sistema; tempo de processamento do evento que levou mais tempo do que o padrão para ser processado pelo Inspetor do Sistema; número total de eventos que demoraram mais tempo do que o tempo padrão para processar pelo Inspetor do Sistema.

- Informações sobre todos os objetos e operações processados: Veredito do software sobre o objeto sendo processado; código do diretório; tamanho do objeto que está sendo processado; soma de verificação (SHA256) do objeto que está sendo processado; número do software detectado no contexto do Inspetor do Sistema; data e hora da detecção do software pelo Inspetor do Sistema; detectar características; ID do registro acionado nos bancos de dados de antivírus do Software; motivo da detecção do software pelo Inspetor do Sistema; soma de verificação (MD5) do objeto que está sendo processado; resultado da verificação de integridade do módulo; nome do objeto que está sendo processado; tipo do registro acionado nos bancos de dados de antivírus do Software; caminho para o objeto que está sendo processado; o nome do objeto verificado; a data e hora da verificação; os endereços URL e de referência dos quais foi baixado; o tamanho dos arquivos verificados e os caminhos para eles; o sinal de arquivo; a data e hora da criação do arquivo; o nome, tamanho e somas de verificação (MD5, SHA2-256) do compactador (se o arquivo foi empacotado); a entropia do arquivo; o tipo de arquivo; o código do tipo de arquivo; o sinal, ID e formato do arquivo executável; a soma de verificação do objeto (MD5, SHA2-256); o tipo e o valor da soma de verificação suplementar do objeto; dados sobre a assinatura digital do objeto (certificado): dados sobre o editor do certificado, número de inicializações do objeto desde a última entrega de estatísticas, ID da tarefa de verificação do aplicativo, meio de recebimento de informações sobre a reputação do objeto, valor do filtro alvo, parâmetros técnicos das tecnologias de detecção aplicáveis; caminho para o objeto que está sendo processado; código do diretório.

- Para arquivos executáveis: a entropia das seções do arquivo, indicador de verificação de reputação ou indicador de assinatura de arquivo, nome, tipo, tipo de ID, soma de verificação (MD5) e o tamanho do aplicativo que foi carregado pelo objeto que está sendo validado, o caminho do aplicativo e os caminhos do modelo, um atributo indicando presença na lista de Autorun, data de entrada, lista de atributos, nome do compactador, informações sobre a assinatura digital do aplicativo: o certificado do editor, o nome do arquivo carregado no formato MIME, a data e hora de compilação do arquivo.

- Informações sobre aplicativos iniciados e os seus módulos: somas de verificação (MD5, SHA2-256) de arquivos em execução, tamanho, atributos, data de criação, nome do compactador (se o arquivo foi compactado), nomes de arquivos, informações sobre processos em execução no sistema (ID do processo (PID)), nome do processo, informações sobre a conta a partir da qual o processo foi iniciado, o aplicativo e o comando que iniciaram o processo, o caminho completo para os arquivos do processo e a linha de comando inicial, uma descrição do aplicativo ao qual o processo pertence (o nome do aplicativo e as informações sobre o editor, além dos certificados digitais usados e as informações necessárias para verificar a autenticidade ou as informações sobre a ausência de assinatura digital de um arquivo), e informações sobre os módulos carregados nos processos: seus nomes, tamanhos, tipos, datas de criação, atributos, somas de verificação (MD5, SHA2-256, SHA1), os caminhos para eles, informações do cabeçalho do arquivo PE, nomes dos compactadores (se o arquivo foi compactado), informações sobre a disponibilidade e validade dessas estatísticas, identificador do modo para gerar as estatísticas que estão sendo enviadas.

- Se forem detectadas ameaças ou vulnerabilidades, além das informações sobre o objeto detectado, são fornecidas informações sobre o identificador, a versão e o tipo do registro no banco de dados de antivírus, o nome da ameaça com base na classificação da Kaspersky, a data e hora da última atualização do banco de dados de antivírus, o nome do arquivo executável, a soma de verificação (MD5) do arquivo do aplicativo que solicitou o URL no qual a ameaça foi detectada, o endereço IP (IPv4 ou IPv6) da ameaça detectada, o identificador de vulnerabilidade e seu nível de ameaça, o URL e o referenciador da página da Web em que a vulnerabilidade foi detectada.

- Se um objeto potencialmente malicioso for detectado, são fornecidas informações sobre os dados na memória dos processos.

- Informações sobre ataque de rede: endereço IP do computador atacante e número da porta no computador do usuário visado pelo ataque de rede, ID do protocolo de ataque, nome e tipo de ataque.

- Informações sobre conexões de rede: versão e somas de verificação (MD5, SHA2-256, SHA1) do arquivo a partir do qual foi iniciado o processo que abriu a porta, caminho para o arquivo do processo e a respectiva assinatura digital, endereços IP local e remoto, número de portas de conexão locais e remotas, estado da conexão, carimbo de data e hora da abertura da porta.

- O URL e o endereço IP da página da Web onde o conteúdo danoso ou suspeito foi detectado, o nome, tamanho e soma de verificação do arquivo que solicitou o URL, o identificador, peso e grau da regra utilizada para obter um veredito, o objetivo do ataque.

- Informações sobre as atualizações do aplicativo instalado e bancos de dados de antivírus: status de conclusão da tarefa de atualização, tipo de erro que pode ter ocorrido durante o processo de atualização, o número de atualizações sem êxito, o identificador do componente do aplicativo que executa as atualizações.

- Informações sobre o uso da Kaspersky Security Network (KSN): identificador da KSN, identificador do aplicativo, versão completa do aplicativo, endereço IP despersonalizado do dispositivo do usuário, indicadores da qualidade do cumprimento das solicitações da KSN, indicadores da qualidade do processamento de pacotes da KSN, indicadores do número de solicitações da KSN e informações sobre os tipos de solicitações da KSN, data e hora do início do envio das estatísticas, data e hora do término do envio das estatísticas, informações sobre as atualizações de configuração da KSN: identificador da configuração ativa, identificador da configuração recebida, código de erro da atualização da configuração.

- Informações sobre eventos de log do sistema: hora do evento, nome do registro onde o evento foi detectado, tipo e categoria do evento, nome da fonte do evento e descrição do evento.

- Informações para determinar a reputação de arquivos e endereços URL: o endereço de URL no qual a reputação está sendo solicitada e o Referenciador, o tipo de protocolo da conexão, o identificador interno do tipo de aplicativo, o número da porta que está sendo utilizada, o identificador de Usuário, a soma de verificação do arquivo verificado (MD5), tipo de ameaça detectada, informações sobre o registro usado para detectar uma ameaça (identificador de registro para os bancos de dados de antivírus, o registro de data e hora e o tipo); chave pública do certificado; impressão digital do certificado digital do objeto verificado e algoritmo de hash.

- Dados sobre a distribuição territorial do aplicativo: data de instalação e ativação do aplicativo, ID do parceiro que fornece a licença para a ativação do aplicativo, ID do aplicativo, ID de localização do idioma do aplicativo, número de série da licença para a ativação do aplicativo, sinal de participação da KSN.

- Informações sobre a licença usada: o tipo e o período de validade da licença, número de dias até a expiração da licença, identificador do parceiro de quem a licença foi adquirida, identificador do Centro de Ativação Regional, soma de verificação do código de ativação, hash do corpo do tíquete calculado usando o algoritmo SHA1, data e hora da criação do tíquete de licença, identificador de informações da licença, identificador do tíquete de licença, identificador da sequência do tíquete de licença, identificador exclusivo do computador do usuário, data a partir da qual o tíquete de licença começa a valer, data de expiração da validade do tíquete de licença, estado atual do tíquete de licença, versão do cabeçalho do tíquete, versão da licença, identificador do certificado de assinatura do cabeçalho do tíquete, soma de verificação do arquivo de chave, número de série do assinante do cabeçalho do tíquete, token de autenticação.

- Informações sobre o hardware instalado no computador: tipo, nome, nome do modelo, versão do firmware, parâmetros de dispositivos integrados e conectados.

- Informações sobre o dispositivo: ID do dispositivo.

- Informações sobre a operação do componente Controle da Web:
  versão do componente, motivo da categorização, informações adicionais sobre o motivo da categorização, URL categorizado, endereço IP do host do objeto bloqueado/categorizado.

Modo de nuvem

O botão de alternância do **Modo de nuvem** ativa/desativa o modo operacional do aplicativo no qual o Kaspersky Endpoint Security usa uma versão light de bancos de dados antimalware. Esse modo está disponível apenas se a participação na Kaspersky Security Network estiver ativada. A versão leve dos bancos de dados antimalware permite o uso de cerca de metade da memória RAM do computador que seria usada com os bancos de dados usuais. Se você não participar da Kaspersky Security Network ou se o modo na nuvem estiver desativado, o Kaspersky Endpoint Security baixará a versão completa dos bancos de dados antimalware dos servidores da Kaspersky.

Se o botão de alternância estiver ativado, o Kaspersky Endpoint Security usará a versão leve dos bancos de dados antimalware, o que reduz a carga nos recursos do sistema operacional.

> **Nota:** o Kaspersky Endpoint Security baixará a versão leve dos bancos de dados antimalware durante a próxima atualização após a caixa de seleção ser marcada.

Se o botão de alternância estiver desativado, o Kaspersky Endpoint Security usará a versão completa dos bancos de dados antimalware.

> **Nota:** o Kaspersky Endpoint Security baixará a versão completa dos bancos de dados antimalware durante a próxima atualização após a caixa de seleção ser desmarcada.

Declaração da KSN

Clicar nesse link abre uma janela na qual é possível ler a Declaração da Kaspersky Security Network e aceitar seus termos de participação.

Nota: se você gerencia o Kaspersky Endpoint Security por meio do Kaspersky Security Center Web Console, dependendo das configurações do Kaspersky Security Center, poderá participar da Kaspersky Private Security Network, em vez da Kaspersky Security Network. Se você gerenciar o Kaspersky Endpoint Security por meio do Kaspersky Security Center Cloud Console, a participação na Kaspersky Private Security Network não estará disponível. Para obter informações detalhadas sobre a participação na Kaspersky Private Security Network, consulte a ajuda do Kaspersky Security Center.

Na seção **Configurações do proxy da KSN**, você pode definir as configurações de proxy da KSN.

Usar proxy da KSN

Esta caixa de seleção ativa/desativa o uso de um servidor proxy ao conectar-se à Kaspersky Security Network.

Se a caixa de seleção estiver marcada, o Kaspersky Endpoint Security usará um servidor proxy para conectar-se à Kaspersky Security Network.

Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security se conectará diretamente à Kaspersky Security Network.

Esta caixa de seleção está desmarcada por padrão.

Usar servidores da Kaspersky quando o proxy da KSN estiver indisponível

Essa caixa de seleção ativa/desativa o uso dos serviços da Kaspersky se o proxy da KSN não estiver disponível.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security usará os servidores da Kaspersky quando o proxy da KSN estiver indisponível.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não usará os servidores da Kaspersky quando o proxy da KSN estiver indisponível.

Esta caixa de seleção está desmarcada por padrão.

Essa caixa de seleção ficará disponível se a opção **Usar proxy da KSN** for marcada.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela “Participação na Kaspersky Security Network/Kaspersky Private Security Network”

Saiba mais

Clicar nesse link abre uma nova janela do navegador, na qual é possível ler o texto da Declaração da Kaspersky Security Network ou da Kaspersky Private Security Network.

Eu aceito os termos de participação na Kaspersky Security Network/Kaspersky Private Security Network

Os computadores nos quais a política é aplicada participam da Kaspersky Security Network/Kaspersky Private Security Network.

Eu não aceito os termos de participação na Kaspersky Security Network/Kaspersky Private Security Network

Os computadores nos quais a política é aplicada não participam da Kaspersky Security Network/Kaspersky Private Security Network.

Nota: se você gerenciar o Kaspersky Endpoint Security por meio do Kaspersky Security Center Cloud Console, a participação na Kaspersky Private Security Network não estará disponível. Para obter informações detalhadas sobre a participação na Kaspersky Private Security Network, consulte a ajuda do Kaspersky Security Center.

A seção Proteção Essencial Contra Ameaças

Proteção Contra Ameaças ao Arquivo

Clicar nesse link abre uma janela na qual é possível definir as Configurações de Proteção Contra Ameaças ao Arquivo.

Proteção Contra Ameaças da Web

Clicar nesse link abre uma janela na qual é possível definir as Configurações de Proteção Contra Ameaças da Web.

Proteção Contra Ameaças à Rede

Clicar nesse link abre uma janela na qual é possível definir as Configurações de Proteção Contra Ameaças à Rede.

Proteção Contra Ameaças ao Correio

Clicar nesse link abre uma janela na qual é possível definir as Configurações de Proteção Contra Ameaças ao Correio.

Firewall

Clicar nesse link abre uma janela na qual é possível definir as configurações de Firewall.

A janela Proteção Contra Ameaças ao Arquivo

Proteção Contra Ameaças ao Arquivo

O botão **Proteção Contra Ameaças ao Arquivo** ativa/desativa a Proteção Contra Ameaças ao Arquivo.

Se o botão **Proteção Contra Ameaças ao Arquivo** estiver ativado, o Kaspersky Endpoint Security realizará um monitoramento em tempo real do sistema de arquivos dos computadores clientes aos quais a política é aplicada.

Se o botão **Proteção Contra Ameaças ao Arquivo** estiver desativado, o Kaspersky Endpoint Security não protegerá o sistema de arquivos dos computadores clientes aos quais a política é aplicada.

Por padrão, esse botão está ativado.

Na seção **Escopo da proteção**, é possível configurar um escopo de proteção selecionando um dos itens predefinidos ou adicionando arquivos ou pastas de sua escolha.

Adicionar

Clicar nesse botão abre uma caixa de diálogo na qual é possível especificar um arquivo, uma pasta ou uma máscara a ser adicionada à lista de objetos incluídos no escopo de proteção.

Excluir

Clicar nesse botão remove um objeto do escopo de proteção.

Este botão ficará disponível se um objeto for selecionado na lista de objetos protegidos.

Você não pode excluir os objetos padrão incluídos no escopo de proteção.

Escopo da proteção

Essa coluna contém os objetos verificados pelo Kaspersky Endpoint Security quando a Proteção Contra Ameaças ao Arquivo estiver ativada.

Por padrão, o Kaspersky Endpoint Security verifica os seguintes objetos:

- **Todos os discos removíveis**. O Kaspersky Endpoint Security verifica todas as unidades removíveis.
- **Todos os discos internos**. O Kaspersky Endpoint Security verifica todas as unidades internas.
- **Todos os discos de rede**. O Kaspersky Endpoint Security verifica todas as unidades de rede.

Status

Se o botão nessa coluna estiver ligado, o Kaspersky Endpoint Security verificará o objeto correspondente na coluna **Escopo da proteção** quando a Proteção Contra Ameaças ao Arquivo estiver ativada.

Se o botão nessa coluna estiver desligado, o Kaspersky Endpoint Security não verificará o objeto correspondente na coluna **Escopo da proteção** quando a Proteção Contra Ameaças ao Arquivo estiver ativada.

Adicional

Essa coluna indica se o Kaspersky Endpoint Security verificará as subpastas do objeto correspondente.

Na seção **Se um objeto malicioso for detectado**, é possível selecionar a ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto malicioso.

Perguntar o que fazer

O Kaspersky Endpoint Security exibe uma janela de notificações com informações sobre o objeto malicioso que infectou o arquivo e solicita que você escolha a ação a ser executada pelo Kaspersky Endpoint Security. As ações disponíveis podem variar dependendo do status do objeto.

Esta opção está marcada por padrão.

Desinfectar, excluir se a desinfecção falhar

O Kaspersky Endpoint Security bloqueia o acesso ao arquivo infectado e tenta desinfectá-lo sem solicitar a confirmação do usuário.

Se a desinfecção for bem-sucedida, o Kaspersky Endpoint Security salvará o arquivo em sua localização original com o nome original do arquivo. Se ocorrer uma falha na desinfecção, o Kaspersky Endpoint Security excluirá o arquivo infectado.

Desinfectar, bloquear se a desinfecção falhar

O Kaspersky Endpoint Security bloqueia o acesso ao arquivo infectado e tenta desinfectá-lo sem solicitar a confirmação do usuário.

Se a desinfecção for bem-sucedida, o Kaspersky Endpoint Security salvará o arquivo em sua localização original com o nome original do arquivo. Se ocorrer falha na desinfecção, o Kaspersky Endpoint Security manterá o arquivo infectado bloqueado e em sua localização original.

Na seção **Otimização**, é possível configurar o desempenho da verificação e selecionar o algoritmo de verificação.

Verificar apenas arquivos novos e modificados

Essa caixa de seleção ativa/desativa a verificação apenas dos arquivos que o Kaspersky Endpoint Security reconhece como novos ou modificados desde a verificação anterior.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará apenas os arquivos que reconhecer como novos ou modificados desde a última verificação.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará todos os arquivos.

Esta caixa de seleção está marcada por padrão.

Ignorar a verificação de volumes de sistema somente leitura

Esta caixa de seleção ativa/desativa a verificação do volume do sistema somente leitura pelo Kaspersky Endpoint Security.

Caso esta caixa de seleção esteja marcada, o Kaspersky Endpoint Security não verificará o volume do sistema em somente leitura. Isso reduz significativamente o tempo de verificação.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará o volume do sistema somente leitura.

Esta caixa de seleção está marcada por padrão.

Usar iSwift

Essa caixa de seleção ativa/desativa o uso da tecnologia iSwift durante a verificação. O iSwift permite que o Kaspersky Endpoint Security use um algoritmo especial para excluir determinados objetos da verificação, o que ajuda a aumentar a velocidade dela.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security usará o iSwift durante a verificação.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não usará o iSwift durante a verificação.

Esta caixa de seleção está marcada por padrão.

Na seção **Tipos de arquivos**, é possível selecionar quais arquivos serão verificados pelo Kaspersky Endpoint Security quando a Proteção Contra Ameaças ao Arquivo estiver ativada.

Verificar todos os arquivos

O Kaspersky Endpoint Security verifica todos os objetos do sistema de arquivos que são executados, abertos ou salvos.

Verificar aplicativos e documentos por conteúdo

O Kaspersky Endpoint Security verifica somente os objetos que podem estar infectados com base em seu conteúdo.

Verificar aplicativos e documentos por extensão

O Kaspersky Endpoint Security verifica somente os objetos que podem estar infectados com base na extensão do arquivo.

A lista de extensões é definida pela Kaspersky e está incluída nos bancos de dados do Kaspersky Endpoint Security.

O Kaspersky Endpoint Security sempre verifica os arquivos sem extensões.

Na seção **Arquivos compostos**, é possível selecionar os tipos de arquivos compostos verificados pelo Kaspersky Endpoint Security quando a Proteção Contra Ameaças ao Arquivo estiver ativada.

Verificar arquivos comprimidos

Esta caixa de seleção ativa/desativa a verificação de arquivos. Para obter a lista de extensões, consulte a Ajuda do Kaspersky Endpoint Security.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará os arquivos.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security ignorará os arquivos durante as verificações.

Verificar pacotes de instalação

Esta caixa de seleção ativa/desativa a verificação de pacotes de instalação.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará os pacotes de instalação.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security ignorará os pacotes de instalação durante as verificações.

Verificar objetos OLE incorporados

Esta caixa de seleção ativa/desativa a verificação de objetos incorporados em um arquivo, como planilhas do Excel, macros ou anexos de e-mail.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará os objetos OLE incorporados.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security ignorará os objetos OLE incorporados durante as verificações.

Não extrair arquivos maiores que MB

Esta caixa de seleção ativa/desativa um limite no tamanho dos arquivos a serem verificados.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security ignorará os arquivos maiores que o valor especificado durante as verificações.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security extrairá e verificará os arquivos independentemente do tamanho.

Essa caixa de seleção ficará disponível se a opção **Verificar arquivos comprimidos** for marcada.

Adiar a extração de arquivos maiores que MB

Uma opção que limita o tamanho dos arquivos a serem verificados.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará todos os arquivos cujo tamanho exceder o limite definido, mas fará isso dois minutos após a detecção desse arquivo comprimido com uma prioridade mais baixa.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará todos os arquivos com a mesma prioridade.

Essa caixa de seleção ficará disponível se a opção **Verificar arquivos comprimidos** for marcada.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A caixa de diálogo “Adicionar escopo da proteção”

Campo de entrada Insira um nome de arquivo, nome de pasta ou máscara

Caminho para um arquivo, uma pasta ou uma máscara de arquivos/ pastas.

O objeto é uma pasta

Esta caixa de seleção ativa/desativa a verificação de um objeto como uma pasta.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará o objeto especificado no campo **Insira um nome de arquivo, nome de pasta ou máscara** como uma pasta.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará o objeto especificado no campo **Insira um nome de arquivo, nome de pasta ou máscara** como um arquivo.

Esta caixa de seleção está marcada por padrão.

Incluir subpastas

Esta caixa de seleção ativa/desativa a verificação de subpastas na pasta especificada no campo **Insira um nome de arquivo, nome de pasta ou máscara**.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará as subpastas durante as verificações de malware.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará apenas os arquivos diretamente na pasta especificada no campo **Insira um nome de arquivo, nome de pasta ou máscara** durante as verificações de malware.

Esta caixa de seleção está marcada por padrão.

A janela “Proteção Contra Ameaças da Web”

Proteção Contra Ameaças da Web

O botão **Proteção Contra Ameaças da Web** ativa/desativa a Proteção Contra Ameaças da Web.

Se o botão **Proteção Contra Ameaças da Web** estiver ativado, a Proteção Contra Ameaças da Web verificará os dados enviados e recebidos pelo computador por meio dos protocolos HTTP e HTTPS no Safari, Google Chrome ou Firefox.

Se o botão **Proteção Contra Ameaças da Web** estiver desativado, a Proteção Contra Ameaças da Web não verificará os dados enviados e recebidos pelo computador por meio de navegadores da Web.

Por padrão, esse botão está ativado.

Na seção **Se um objeto malicioso for detectado**, é possível selecionar a ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto malicioso.

Perguntar o que fazer

O Kaspersky Endpoint Security exibe uma janela de notificações com informações sobre o tipo de malware que infetou o objeto de tráfego da Web e solicita que você selecione a ação que deseja que o Kaspersky Internet Security execute nesse objeto. As ações disponíveis podem variar dependendo do status do objeto.

Esta ação está selecionada por padrão.

Bloquear automaticamente

O Kaspersky Endpoint Security bloqueia automaticamente o acesso a objetos de tráfego da Web perigosos.

Na seção **Endereços da Web confiáveis**, é possível criar ou editar uma lista de endereços da Web confiáveis e ativar ou desativar a verificação de tráfego a partir de endereço da Web nessa lista.

Não verificar tráfego da Web de endereços da Web confiáveis

Esta caixa de seleção ativa/desativa a verificação do tráfego de endereços da Web confiáveis.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security não verificará o tráfego de endereços da Web confiáveis.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará o tráfego de endereços da Web confiáveis.

Esta caixa de seleção está desmarcada por padrão.

Lista de endereços da Web

Esta lista contém os endereços da Web confiáveis.

Você pode desmarcar a caixa de seleção ao lado de um endereço da Web na lista. Se a caixa de seleção estiver desmarcada, a Proteção Contra Ameaças da Web verificará o tráfego do endereço da Web.

Esta lista ficará disponível se a caixa de seleção **Não verificar tráfego da Web de endereços da Web confiáveis** for marcada.

Adicionar

Clicar nesse botão abre uma caixa de diálogo na qual é possível inserir um endereço da Web ou uma máscara de endereços da Web a ser adicionada à lista de endereços da Web confiáveis.

Excluir

Clicar neste botão remove o endereço da Web ou a máscara de endereços da Web da lista.

Este botão ficará disponível quando um endereço da Web ou uma máscara de endereços da Web for selecionada na lista de endereços da Web confiáveis.

Endereço da Web

Essa coluna contém os endereços da Web confiáveis.

Status

Se o botão nessa coluna estiver ligado, o Kaspersky Endpoint Security não verificará o objeto correspondente na coluna **Endereço da Web**, quando a Proteção Contra Ameaças da Web estiver ativada e a caixa de seleção **Não verificar tráfego da Web de endereços da Web confiáveis** estiver marcada.

Se o botão nessa coluna estiver desligado, o Kaspersky Endpoint Security verificará o objeto correspondente na coluna **Endereço da Web**, quando a Proteção Contra Ameaças da Web estiver ativada, e a caixa de seleção **Não verificar tráfego da Web de endereços da Web confiáveis** estiver marcada.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A caixa de diálogo “Adicionar endereço da Web”

Campo de entrada Endereço da Web

Um endereço da Web ou a máscara de endereços da Web cujo tráfego não será verificado pela Proteção Contra Ameaças da Web.

Na seção **Status**, é possível definir se o Kaspersky Endpoint Security verificará o tráfego do endereço da Web ou do grupo de endereços da Web.

Desativar

O endereço da Web ou a máscara de endereço da Web é adicionada à lista de **Endereços da Web confiáveis**, mas o Kaspersky Endpoint Security verificará o tráfego.

Ativar

O endereço da Web ou a máscara de endereço da Web é adicionada à lista de **Endereços da Web confiáveis** e o Kaspersky Endpoint Security não verificará o tráfego.

A janela “Proteção Contra Ameaças à Rede”

Proteção Contra Ameaças à Rede

O botão **Proteção Contra Ameaças à Rede** ativa/desativa a Proteção Contra Ameaças à Rede.

Se o botão **Proteção Contra Ameaças à Rede** estiver ativado, o Kaspersky Endpoint Security protegerá o computador remoto contra ataques à rede.

Se o botão **Proteção Contra Ameaças à Rede** estiver desativado, o Kaspersky Endpoint Security não protegerá o computador remoto contra ataques à rede.

Por padrão, esse botão está ativado.

Na seção **Configurações de Proteção Contra Ameaças à Rede**, é possível alterar o período pelo qual o Kaspersky Endpoint Security bloqueará os computadores invasores.

Bloquear computadores responsáveis pelo ataque por min

Esta caixa de seleção ativa/desativa a adição de computadores responsáveis pelo ataque à lista de computadores bloqueados pelo período especificado.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security adicionará os computadores responsáveis pelo ataque à lista de computadores bloqueados pelo período especificado.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não bloqueará os computadores responsáveis pelo ataque.

Esta caixa de seleção está marcada por padrão.

Por padrão, os computadores invasores são bloqueados por 60 minutos.

Na seção **Exclusões**, é possível criar ou editar uma lista de endereços IP de computadores remotos cujas atividades de rede nunca serão bloqueadas pelo Kaspersky Endpoint Security.

Lista de endereços IP

Esta lista contém os endereços IP de computadores remotos cujas atividades de rede nunca serão bloqueadas pelo Kaspersky Endpoint Security.

Adicionar

Clicar nesse botão abre uma caixa de diálogo na qual é possível inserir o endereço IP de um computador remoto.

Excluir

Clicar neste botão remove o endereço IP selecionado da lista.

Este botão ficará disponível se o endereço IP de um computador remoto for selecionado na lista de endereços IP.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A caixa de diálogo “Adicionar exclusão”

Campo de entrada Endereço IP

Endereço IP de um computador remoto.

A seção “Controles de Segurança”

Controle da Web

O botão **Controle da Web** ativa/desativa o Controle da Web.

Se o botão **Controle da Web** estiver ativado, é possível criar regras para gerenciar sites visitados pelos usuários em computadores remotos.

Se o botão **Controle da Web** estiver desativado, não é possível gerenciar sites visitados pelos usuários em computadores remotos.

Por padrão, esse botão está desativado.

Lista de regras

Esta lista contém regras criadas para gerenciar sites visitados por usuários em computadores remotos.

A ordem em que as regras são classificadas determina a prioridade de sua aplicação pelo Kaspersky Endpoint Security.

Adicionar

Clicar neste botão abre uma janela na qual você pode criar uma nova regra para o Controle da Web.

Excluir

Clicar nesse botão remove a regra selecionada da lista de regras.

Esse botão ficará disponível se a caixa de seleção ao lado da regra estiver marcada.

Para cima

Clicar nesse botão move a regra selecionada para cima na lista de regras e aumenta a prioridade de sua aplicação pelo Kaspersky Endpoint Security.

Para baixo

Clicar nesse botão move a regra selecionada para baixo na lista de regras e diminui a prioridade de sua aplicação pelo Kaspersky Endpoint Security.

Nome

O nome da regra.

Estado

O botão nesta coluna define se a regra está ou não ativa.

É possível ativar/desativar o botão ao lado de uma regra correspondente para alterar o estado da regra.

Ação

Uma ação executada pelo Kaspersky Endpoint Security quando o usuário visita um determinado endereço da Web, um grupo de endereços da Web ou uma categoria de sites afetada pela regra.

É possível alterar a ação atribuída selecionando outra opção no menu de atalho correspondente na coluna.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela “Editar regra”

Campo de entrada Nome da regra

O nome da regra.

Na seção **Estado**, é possível definir a regra como ativa ou inativa.

Ativo

Se esta opção estiver selecionada, você criará uma regra ativa. Ela será aplicada ao computador remoto logo após a aplicação da política.

Inativo

Se esta opção estiver selecionada, você criará uma regra inativa. Ela estará pendente quando a política for aplicada.

Na seção **Ação**, é possível selecionar a ação que o Kaspersky Endpoint Security deve executar quando o usuário visitar um determinado endereço da Web, um grupo de endereços da Web ou uma categoria de sites afetada pela regra.

Permitir

Se esta opção estiver selecionada, o Kaspersky Endpoint Security permitirá que o usuário visite o endereço da Web, o grupo de endereços da Web ou a categoria de sites afetada pela regra.

Nota: caso o botão de alternância **Verificar conexões seguras (HTTPS)** esteja ligado na janela **Rede** do assistente para Novas Políticas, o Kaspersky Endpoint Security permitirá visitar os recursos da Web no computador remoto.

Esta opção está marcada por padrão.

Bloquear

Se esta opção estiver selecionada, o Kaspersky Endpoint Security impedirá que o usuário visite o endereço da Web, o grupo de endereços da Web ou a categoria de sites afetada pela regra.

Nota: caso o botão de alternância **Verificar conexões seguras (HTTPS)** esteja ativado na janela **Rede** do Assistente para Novas Políticas, o Kaspersky Endpoint Security exibirá notificações quando o usuário acessar os recursos da Web bloqueados pelo Controle da Web no computador remoto.

Exibir aviso

Se esta opção estiver selecionada, o Kaspersky Endpoint Security exibirá um aviso quando o usuário tentar visitar o endereço da Web, o grupo de endereços da Web ou a categoria de sites afetada pela regra.

Na seção **Área da regra**, é possível optar por criar uma regra para um endereço da Web específico ou para um grupo de endereços da Web ou categorias de site.

Categorias

Se esta opção estiver selecionada, você criará uma regra para as categorias de sites.

Selecionar categorias

Clicar nesse link abre a caixa de diálogo na qual é possível selecionar categorias de site afetadas pela regra.

Endereços individuais

Se esta opção estiver selecionada, você criará uma regra para um endereço da Web específico ou um grupo de endereços da Web.

Esta opção está marcada por padrão.

Adicionar

Clicar nesse botão abre uma caixa de diálogo na qual é possível especificar um endereço da Web ou uma máscara de endereços da Web afetada pela regra.

Excluir

Clicar nesse botão remove o endereço da Web ou a máscara de endereços da Web selecionada da lista de endereços da Web afetados pela regra.

Esse botão ficará disponível se a caixa de seleção ao lado do endereço da Web da máscara de endereços da Web estiver marcada.

Endereço

Endereços da Web ou máscaras de endereços da Web afetadas pela regra.

A caixa de diálogo “Adicionar endereço da Web”

Campo de entrada Endereço da Web

O endereço da Web ou a máscara de endereços da Web que será afetada pela regra.

A caixa de diálogo “Categorias de conteúdo”

Lista das categorias de conteúdo

Esta lista contém a lista de categorias de sites que você pode adicionar à regra.

A caixa de seleção ao lado do nome da categoria de um site adiciona/remove os sites que pertencem a essa categoria para a/da regra.

Todas as caixas de seleção estão desmarcadas por padrão.

A seção Detection and Response

Managed Detection and Response

Ao clicar neste link, uma janela na qual é possível definir as configurações do Managed Detection and Response é aberta.

Endpoint Detection and Response

Ao clicar neste link, uma janela na qual é possível definir as configurações do Endpoint Detection and Response é aberta.

Endpoint Detection and Response Expert (on-premise)

Clicar neste link abre uma janela onde você pode definir as configurações do Endpoint Detection and Response Expert (on-premise).

A janela “Managed Detection and Response”

Managed Detection and Response

O botão do **Managed Detection and Response** ativa/desativa o componente Managed Detection and Response que interage com o serviço Kaspersky Managed Detection and Response. Esse serviço detecta e elimina constantemente ameaças à segurança da sua organização.

Se o botão de alternância **Managed Detection and Response** estiver ativado e o arquivo de configuração do MDR tiver sido importado, o componente Managed Detection and Response estará ativado.

Se o botão do **Managed Detection and Response** estiver desativado, o componente Managed Detection and Response estará desativado.

Por padrão, esse botão está desativado.

Importar

Clicar nesse botão abre a janela que permite importar o arquivo de configuração do MDR na política do Kaspersky Endpoint Security.

Excluir o arquivo de configuração

Ao clicar no botão, o arquivo de configuração do MDR é excluído da política do Kaspersky Endpoint Security.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela Endpoint Detection and Response

Endpoint Detection and Response

O botão de alternância do **Endpoint Detection and Response** ativa/desativa o componente Endpoint Detection and Response que interage com a solução Kaspersky Endpoint Detection and Response. Essa solução protege os computadores contra ameaças complicadas, inclusive as novos exploits, ransomwares e ataques sem arquivo.

Caso o botão de alternância do **Endpoint Detection and Response** esteja ativado, o componente Endpoint Detection and Response estará ativado.

Caso o botão de alternância do **Endpoint Detection and Response** esteja desativado, o componente Endpoint Detection and Response estará desativado.

Por padrão, esse botão está desativado.

Na seção **Isolamento de rede**, é possível definir os ajustes para isolar os computadores da rede em resposta à detecção de um indicador de comprometimento.

Definir os ajustes de desbloqueio do computador

Clicar nesse link abre uma janela onde é possível especificar o atraso para desativar automaticamente o isolamento de rede.

Exclusões

Clicar nesse link abre uma janela onde é possível especificar as conexões de rede que não são bloqueadas no computador depois que o isolamento de rede é ativado automaticamente.

Na seção **Prevenção de execução**, é possível definir os ajustes para a execução de arquivos executáveis, scripts e a abertura de arquivos no formato Office.

Prevenção de execução

O botão de alternância **Prevenção de execução** ativa/desativa a prevenção de execução.

Caso o botão de alternância **Prevenção de execução** esteja ativado, será possível criar e editar a lista de regras de prevenção de execução e selecionar uma ação a ser executada quando os objetos proibidos forem executados ou abertos.

Caso a opção **Prevenção de execução** esteja desativada, não será possível gerenciar os objetos que os usuários executam ou abrem em seus dispositivos.

Por padrão, esse botão está desativado.

Ação na execução ou abertura de objeto proibido

Bloquear e gravar no relatório

Caso esse modo seja selecionado, o aplicativo bloqueará a execução de objetos ou a abertura de documentos que atendem aos critérios da regra de prevenção. O aplicativo também publica um evento sobre tentativas de executar objetos ou abrir documentos no log de eventos do Kaspersky Security Center e no sistema de login unificado.

Criar log de eventos apenas

Caso esse modo seja selecionado, o Kaspersky Endpoint Security publicará um evento sobre as tentativas de execução de objetos executáveis ou documentos abertos que correspondam aos critérios da regra de prevenção no log de eventos do Kaspersky Security Center e no sistema de login unificado, mas não bloqueará a tentativa de execução ou abertura do objeto ou documento. Este modo está marcado por padrão.

Adicionar

Clicar nesse botão abre uma caixa de diálogo onde é possível criar uma novas regras de prevenção de execução.

Editar

Clicar nesse botão abre uma caixa de diálogo na qual é possível editar regras de prevenção de execução.

Esse botão ficará disponível se a regra for selecionada na lista de regras.

Excluir

Clicar nesse botão remove uma regra de prevenção de execução selecionada da lista de regras.

Esse botão ficará disponível se a regra for selecionada na lista de regras.

Na seção **Configurações do Cloud Sandbox**, é possível ativar ou desativar o componente Cloud Sandbox.

Cloud Sandbox

O botão de alternância **Cloud Sandbox** ativa/desativa a tecnologia Cloud Sandbox que ajuda a detectar ameaças avançadas em um computador. O Kaspersky Endpoint Security encaminha automaticamente arquivos detectados para a Cloud Sandbox analisar. O Cloud Sandbox executa esses arquivos em um ambiente isolado para identificar atividades maliciosas e avaliar a sua reputação. Os dados nesses arquivos são então enviados para a Kaspersky Security Network. Portanto, caso o Cloud Sandbox detecte um arquivo malicioso, o Kaspersky Endpoint Security executará a ação pertinente para eliminar essa ameaça em todos os computadores onde esse arquivo for detectado.

Caso o botão de alternância do **Cloud Sandbox** esteja ativado, a tecnologia Cloud Sandbox será ativada.

Caso o botão de alternância do **Cloud Sandbox** esteja desligado, a tecnologia Cloud Sandbox será desativada.

Por padrão, esse botão está desativado.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela Ajustes de desbloqueio do computador

Desbloquear automaticamente o computador isolado em

Esta caixa de seleção ativa/desativa o desligamento automático do isolamento de rede após um tempo especificado.

Caso esta caixa de seleção esteja marcada, será possível especificar o atraso para desativar automaticamente o isolamento de rede de um computador.

Caso esta caixa de seleção esteja desmarcada, o Kaspersky Endpoint Security desativará o isolamento de rede o horas após o início do isolamento.

Esta caixa de seleção está marcada por padrão.

Horas

O intervalo após o qual o isolamento de rede será desativado automaticamente.

Este campo estará disponível para edição somente se a caixa de seleção **Desbloquear automaticamente o computador isolado em** estiver marcada.

A janela Exclusões de isolamento de rede

Exclusões de isolamento de rede

Esta lista contém as conexões de rede que foram adicionadas como Exclusões de isolamento de rede.

Adicionar

Clicar nesse botão abre uma janela onde é possível especificar manualmente os ajustes da conexão de rede a serem adicionadas como uma exclusão.

Adicionar a partir do perfil

Clicar nesse botão abre uma janela onde é possível selecionar os perfis de rede padrões para configurar as exclusões.

Excluir

Clicar nesse botão remove uma conexão de rede da lista de Exclusões de isolamento de rede.

Esse botão ficará disponível se um servidor for selecionado na lista de Exclusões de isolamento de rede.

A janela Propriedades da regra

Nome da regra

Nome de uma regra de exclusão de isolamento de rede.

Este é um parâmetro opcional.

Direção

Direção do tráfego.

Protocolo

Tipo de protocolo.

Número

Número do protocolo.

O valor deve estar em conformidade com a lista da IANA para números de protocolo da Internet atribuídos.

Esse campo estará disponível caso o tipo de protocolo **Personalizado** seja selecionado.

Porta local ou intervalo

Porta local ou intervalo do computador para o qual as Exclusões de isolamento de rede estão sendo configuradas.

Porta remota ou intervalo

Porta remota ou intervalo do computador para o qual as Exclusões de isolamento de rede estão sendo configuradas.

Endereço remoto

Endereço de rede do computador para o qual as Exclusões de isolamento de rede estão sendo configuradas.

Aplicativos

Essa caixa permite adicionar um aplicativo que tem permissão para iniciar uma conexão de rede adicionada nas Exclusões de isolamento de rede no computador isolado.

Caso essa caixa esteja marcada, será possível adicionar o aplicativo.

Se essa caixa estiver desmarcada, uma conexão de rede adicionada nas Exclusões de isolamento de rede pode ser iniciada por qualquer aplicativo no computador isolado.

Esta caixa de seleção está desmarcada por padrão.

Adicionar

Clicar nesse botão abre uma janela onde é possível especificar um caminho para um aplicativo que tem permissão para iniciar uma conexão de rede adicionada nas Exclusões de isolamento de rede.

Editar

Clicar nesse botão abre uma janela onde é possível editar um caminho para um aplicativo adicionado.

Esse botão ficará disponível se um aplicativo for selecionado na lista.

Excluir

Clique nesse botão para excluir um aplicativo adicionado.

Esse botão ficará disponível se um aplicativo for selecionado na lista.

A janela Regra de prevenção

Nome

O nome da regra.

Tipo

Tipo de objeto que você deseja bloquear.

Na seção **Caminho para o objeto**, você pode selecionar se deseja especificar o caminho completo para o objeto a ser proibido. Caso opte pela especificação do caminho, insira o valor no campo correspondente.

Na seção **Checksum do objeto**, você pode selecionar se deseja especificar a soma de verificação para o objeto a ser proibido. Caso opte pela especificação da soma de verificação, selecione o tipo e insira o valor no campo correspondente.

A janela Endpoint Detection and Response (KATA)

Endpoint Detection and Response Expert (on-premise)

O botão de alternância **Endpoint Detection and Response Expert (on-premise)** ativa/desativa o componente Endpoint Detection and Response Expert (on-premise) que interage com a solução Kaspersky Anti Targeted Attack Platform. Essa solução detecta prontamente as ameaças avançadas, como ataques direcionados, ameaças persistentes avançadas, ataques de dia zero e outras.

Caso o botão de alternância do **Endpoint Detection and Response Expert (on-premise)** esteja ativado, o componente Endpoint Detection and Response Expert (on-premise) estará ativado.

Caso o botão de alternância do **Endpoint Detection and Response Expert (on-premise)** esteja desativado, o componente Endpoint Detection and Response Expert (on-premise) estará desativado.

Por padrão, esse botão está desativado.

Endpoint Detection and Response Expert (versão 7.1 ou anterior)

Caso esta opção seja selecionada, o componente Endpoint Detection and Response Expert (on-premise) operará no modo de compatibilidade com o Endpoint Detection and Response Expert (versão 7.1 ou anterior).

Endpoint Detection and Response Expert (versão 8.0 ou posterior)

Caso esta opção esteja selecionada, o componente Endpoint Detection and Response Expert (on-premise) opera no modo de compatibilidade com o Endpoint Detection and Response Expert (versão 8.0 ou posterior).

Herdar configurações de conexão da política

Caso esta opção esteja selecionada, as configurações de conexão com servidores de coleta de telemetria, os servidores de coleta de telemetria, as configurações de transmissão de dados de servidores de coleta de telemetria, os limites no número de eventos enviados para os servidores de coleta de telemetria, as configurações de conexão com servidores de resposta e servidores de resposta são herdados da política principal e ficam indisponíveis para edição.

Esta opção estará disponível se o modo **Endpoint Detection and Response Expert (versão 8.0 ou posterior)** for selecionado.

Esta opção está marcada por padrão.

Usar configurações de conexão personalizadas

Caso esta opção esteja selecionada, as configurações de conexão com servidores de coleta de telemetria, os servidores de coleta de telemetria, as configurações de transmissão de dados de servidores de coleta de telemetria, os limites no número de eventos enviados para os servidores de coleta de telemetria, as configurações de conexão com servidores de resposta e servidores de resposta não são herdados da política principal e permanecem disponíveis para edição.

Esta opção estará disponível se o modo **Endpoint Detection and Response Expert (versão 8.0 ou posterior)** for selecionado.

Dependendo do modo selecionado na seção **Conexão com os servidores KATA** ou seção **Conexão com os servidores de coleta de telemetria**, é possível definir as configurações de conexão com os servidores.

Configurações de conexão

Ao clicar neste link, uma caixa de diálogo na qual é possível definir as configurações para conexão com os servidores é aberta.

Enviar solicitação de sincronização para o servidor a cada (min)

O intervalo entre as solicitações de sincronização enviadas a um servidor KATA.

O valor padrão é de 5 minutos.

Esta opção estará disponível se o modo **Endpoint Detection and Response Expert (versão 8.0 ou posterior)** for selecionado.

Adicionar

Clicar neste botão abrirá uma janela onde é possível configurar uma conexão com um servidor.

Editar

Clicar neste botão abrirá uma janela onde é possível editar uma conexão existente com um servidor.

Esse botão ficará disponível se um servidor for selecionado na lista de servidores.

Excluir

Clicar neste botão removerá o servidor selecionado da lista.

Este botão ficará disponível se um servidor for selecionado na lista.

Endereço

Endereço IP de um servidor.

Porta

Número da porta de um servidor.

Na seção **Configurações de transmissão de dados**, é possível definir as configurações para enviar dados para servidores.

Enviar telemetria para KATA

Esta caixa de seleção ativa/desativa o envio de eventos para o servidor KATA.

Caso esta caixa de seleção esteja marcada, os eventos serão enviados ao servidor KATA.

Caso esta caixa de seleção esteja desmarcada, os eventos não serão enviados ao servidor KATA.

Esta opção estará disponível se o modo **Endpoint Detection and Response Expert (versão 7.1 ou anterior)** estiver selecionado.

Essa caixa vem desmarcada por padrão.

Enviar telemetria para os servidores de coleta de telemetria

Esta caixa de seleção ativa/desativa o envio de eventos para o servidor de coleta de telemetria.

Caso esta caixa de seleção esteja marcada, os eventos serão enviados ao servidor de coleta de telemetria.

Caso esta caixa de seleção esteja desmarcada, os eventos não serão enviados ao servidor de coleta de telemetria.

Esta caixa de seleção estará disponível se o modo **Endpoint Detection and Response Expert (versão 8.0 ou posterior)** estiver selecionado.

Essa caixa vem desmarcada por padrão.

Atraso máximo de transmissão de eventos (s)

O intervalo no qual o Kaspersky Endpoint Security envia eventos para um servidor.

O valor padrão é 30 segundos.

Na seção **Limitação de solicitações**, é possível restringir o número de eventos transmitidos.

Ativar a limitação de solicitações

Essa caixa de seleção ativa/desativa a restrição no número de eventos enviados pelo Kaspersky Endpoint Security para um servidor KATA.

Se essa caixa de seleção estiver marcada, o número de eventos enviados pelo aplicativo estará restrito.

Se essa caixa de seleção estiver desmarcada, o número de eventos enviados pelo aplicativo não estará restrito.

Esta caixa de seleção está marcada por padrão.

Número máximo de eventos por hora

O número máximo de eventos que o Kaspersky Endpoint Security envia para um servidor KATA por hora. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora.

O valor padrão é 3000 eventos por hora.

Porcentagem de excesso de limite de evento

O limite para eventos do mesmo tipo (em porcentagem).

O Kaspersky Endpoint Security restringe a transmissão de eventos de um tipo específico se a proporção de eventos desse tipo em relação ao número total de eventos exceder o limite configurado.

O valor padrão é de 15 por cento.

Na seção **Conexão com os servidores de resposta**, é possível definir a as configurações de conexão com os servidores de resposta.

Configurações de conexão

Ao clicar neste link, uma caixa de diálogo na qual é possível definir as configurações para conexão com os servidores é aberta.

Enviar solicitação de sincronização para o servidor a cada (min)

O intervalo entre as solicitações de sincronização enviadas a um servidor KATA.

O valor padrão é de 5 minutos.

Esta opção estará disponível se o modo **Endpoint Detection and Response Expert (versão 8.0 ou posterior)** for selecionado.

Adicionar

Clicar neste botão abrirá uma janela onde é possível configurar uma conexão com um servidor.

Editar

Clicar neste botão abrirá uma janela onde é possível editar uma conexão existente com um servidor.

Esse botão ficará disponível se um servidor for selecionado na lista de servidores.

Excluir

Clicar neste botão removerá o servidor selecionado da lista.

Este botão ficará disponível se um servidor for selecionado na lista.

Endereço

Endereço IP de um servidor.

Porta

Número da porta de um servidor.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela Servidor KATA

Endereço

Endereço IP de um servidor KATA.

Porta

Número da porta de um servidor KATA.

O valor padrão é 443.

A janela Configurações de conexão do servidor

Tempo esgotado (s)

O tempo limite de resposta do servidor KATA. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta se conectar a um servidor KATA diferente.

O valor padrão é 10 segundos.

Na seção **Certificado TLS do servidor**, é possível adicionar ou remover um certificado TLS e visualizar informações sobre o certificado adicionado.

Adicionar certificado TLS

Clicar nesse botão abre uma janela onde é possível selecionar um certificado TLS que será usado para estabelecer uma conexão confiável com um servidor KATA.

Remover

Clicar nesse botão remove o certificado TLS atual.

Esse botão estará disponível se um certificado TLS tiver sido adicionado.

Na seção **Segurança adicional da conexão**, é possível configurar a proteção aprimorada para a conexão entre o Kaspersky Endpoint Security e um servidor KATA.

Usar autenticação de duas etapas

Essa caixa de seleção ativa/desativa a verificação bidirecional que torna a conexão entre o Kaspersky Endpoint Security e um servidor KATA mais segura. Para usar a verificação bidirecional, será necessário carregar um contêiner de criptografia.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security usará a verificação bidirecional para se conectar a um servidor KATA.

Se esta caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não usará a verificação bidirecional para se conectar com um servidor KATA.

Esta caixa de seleção está desmarcada por padrão.

Carregar contêiner de criptografia

Clicar nesse botão abre uma janela onde é possível selecionar o contêiner de criptografia que será usado para verificação bidirecional. O arquivo de contêiner de criptografia tem a extensão .PFX.

Nota: o contêiner de criptografia deve ser protegido por senha. Não é possível adicionar um contêiner de criptografia com uma senha em branco.

Senha do contêiner de criptografia

A senha do contêiner de criptografia usado para verificação bidirecional.

A seção “Atualização”

Atualizar módulos do aplicativo

Esta caixa de seleção ativa/desativa as atualizações dos módulos do aplicativo. Os bancos de dados do aplicativo são sempre atualizados.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security atualizará os módulos do aplicativo.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não atualizará os módulos do aplicativo.

Esta caixa de seleção está marcada por padrão.

Fontes de atualização

Essa lista contém os endereços dos recursos usados pelo Kaspersky Endpoint Security para baixar e instalar as atualizações dos bancos de dados e módulos do aplicativo. Você pode especificar uma pasta local ou de rede, ou um servidor FTP ou HTTP, como uma fonte de atualização.

Por padrão, a lista de fontes de atualização contém os Servidores de atualização Kaspersky.

Se você gerenciar o Kaspersky Endpoint Security por meio do Kaspersky Security Center Web Console, a lista de fontes de atualização também incluirá, por padrão, os servidores do Kaspersky Security Center.

Se você gerenciar o Kaspersky Endpoint Security por meio do Kaspersky Security Center Cloud Console, a lista de fontes de atualização também incluirá, por padrão, os pontos de distribuição. Para obter informações detalhadas sobre os pontos de distribuição, consulte a ajuda do Kaspersky Security Center.

Não é possível remover as fontes de atualização padrão da lista.

Adicionar

Clicar nesse botão abre uma caixa de diálogo na qual é possível especificar o caminho para uma pasta local ou de rede ou um endereço da Web a ser adicionado à lista de fontes de atualização.

Excluir

Clicar nesse botão remove a fonte de atualização selecionada da lista.

Esse botão ficará disponível se a caixa de seleção ao lado da fonte de atualização estiver marcada.

Fonte de atualização

Essa coluna contém fontes de atualização para o Kaspersky Endpoint Security.

Status

Se o botão nessa coluna estiver ligado, o Kaspersky Endpoint Security usará a fonte de atualização correspondente da coluna **Fonte de atualização** para receber atualizações.

Se o botão nessa coluna estiver desligado, o Kaspersky Endpoint Security não usará a fonte de atualização correspondente da coluna **Fonte de atualização** para receber atualizações.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A caixa de diálogo "Adicionar fonte de atualização"

Campo de entrada Insira um caminho para uma pasta de rede ou local, ou um endereço da web

Endereço do recurso do qual o Kaspersky Endpoint Security copia as atualizações.

Você pode especificar um caminho para uma pasta local ou de rede, ou o endereço da Web ou o endereço IP de um servidor FTP ou HTTP, como o endereço do recurso.

Você pode especificar o endereço da web de um servidor FTP no seguinte formato: ftp://<nome do usuário>:<senha>@<host>:<porta>.

Na seção **Status**, é possível definir se o Kaspersky Endpoint Security usará o endereço da Web especificado como uma fonte de atualização.

Desativado

O endereço da Web é adicionado à lista de fontes de atualização, mas o Kaspersky Endpoint Security não o utiliza como fonte de atualização.

Ativado

O endereço da Web é adicionado à lista de fontes de atualização e o Kaspersky Endpoint Security utiliza-o como fonte de atualização.

A seção “Criptografia de Dados”

Criptografia de disco FileVault

O botão **Criptografia de disco FileVault** ativa/desativa o gerenciamento de criptografia de disco FileVault.

Se o botão **Criptografia de disco FileVault** estiver ativado, a criptografia de disco FileVault poderá ser aplicada aos computadores clientes do Kaspersky Security Center.

Se o botão **Criptografia de disco FileVault** estiver desativado, a criptografia de disco FileVault não poderá ser aplicada aos computadores clientes do Kaspersky Security Center.

Por padrão, esse botão está desativado.

Nota: se o botão **Criptografia de disco FileVault** estiver desativado, os usuários com direitos de administrador poderão criptografar e descriptografar os discos de inicialização do Mac no Ajuste do Sistema. Para obter mais informações sobre o FileVault, consulte a documentação da Apple.

Criptografar disco

O Kaspersky Endpoint Security exibe um prompt para obter as credenciais da conta nos computadores clientes aos quais a política é aplicada. Quando o usuário insere as credenciais, o Kaspersky Endpoint Security inicia a criptografia do disco de inicialização do usuário.

Se o botão **Criptografia de disco FileVault** estiver ligado, e a opção **Criptografar disco** estiver selecionada, os usuários com direitos de administrador não poderão descriptografar o disco de inicialização do Mac no Ajuste do Sistema.

Descriptografar disco

O Kaspersky Endpoint Security exibe um prompt para obter as credenciais da conta nos computadores clientes aos quais a política é aplicada. Quando o usuário insere as credenciais, o Kaspersky Endpoint Security inicia a descriptografia do disco de inicialização do usuário.

Se o botão **Criptografia de disco FileVault** estiver ligado, e a opção **Descriptografar disco** estiver selecionada, os usuários com direitos de administrador não poderão criptografar o disco de inicialização do Mac no Ajuste do Sistema.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela Configurações de telemetria

Adicionar

Clicar neste botão abre uma janela onde é possível adicionar uma regra na Zona Confiável.

Editar

Clicar neste botão abre uma janela onde é possível editar a regra selecionada.

Excluir

Clicar neste botão remove a regra selecionada da Zona Confiável.

Status

O botão de alternância nesta coluna ativa/desativa a regra adicionada na Zona confiável.

Caso o botão de alternância esteja ativado, a regra estará ativa.

Caso o botão de alternância esteja desativado, a regra estará inativa.

Nome da regra

Esta coluna contém nomes de regras adicionados na Zona Confiável.

Descrição

Um comentário com informações sobre a regra adicionada na Zona Confiável.

A janela Adicionar/editar regra de exclusão

Status

Esta opção ativa/desativa a regra adicionada na Zona Confiável.

Caso o botão de alternância esteja ativado, a regra estará ativa.

Caso o botão de alternância esteja desativado, a regra estará inativa.

Nome da regra

Nome da regra adicionada na Zona Confiável.

Descrição

Um comentário com informações sobre a regra adicionada na Zona Confiável.

Indicadores de ataque (IOA)

Campo para inserir GUIDs de indicadores de ataque.

A seção Configurações adicionais

Proteção

Ao clicar nesse link, a janela **Proteção** será aberta, na qual é possível gerenciar as configurações gerais do Kaspersky Endpoint Security instalado nos computadores dos usuários e selecionar os tipos de objetos detectados por ele.

Relatórios e backup

Ao clicar nesse link, a janela **Relatórios e backup** será aberta, na qual é possível gerenciar os relatórios as configurações de backup.

Interação do usuário

Ao clicar nesse link, a janela **Interação do usuário** será aberta, na qual é possível configurar as notificações apresentadas pelo Kaspersky Endpoint Security, o idioma de exibição dos eventos demonstrados no Kaspersky Security Center e as configurações adicionais para Kaspersky Endpoint Security.

Rede

Clicar nesse link abre a janela **Rede**, onde você pode gerenciar os ajustes do servidor proxy, ativar ou desativar a verificação de conexões criptografadas (HTTPS), selecionar o armazenamento de certificado para verificar o tráfego HTTPS criptografado no navegador Mozilla Firefox e configurar portas monitoradas.

Zona confiável

Ao clicar nesse link, a janela **Zona confiável** é aberta. Nela, é possível adicionar exclusões para a Proteção Contra Ameaças ao Arquivo ou as tarefas de verificação e configurar aplicativos confiáveis.

A janela Proteção

Na seção **Geral**, você pode ativar ou desativar a proteção de arquivos em um computador remoto e configurar o início automático do aplicativo quando o computador for ligado ou o sistema operacional for reiniciado.

Iniciar o aplicativo na inicialização do computador

Esta caixa de seleção ativa/desativa o início automático do Kaspersky Endpoint Security quando um computador remoto é ligado ou após a reinicialização do sistema operacional.

Se a caixa de seleção estiver marcada, o Kaspersky Endpoint Security iniciará automaticamente quando o computador remoto for ligado ou o sistema operacional for reiniciado.

Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não será iniciado automaticamente quando o computador remoto for ligado ou o sistema operacional for reiniciado.

Esta caixa de seleção está marcada por padrão.

Importante: se você marcar esta caixa de seleção quando o Kaspersky Endpoint Security não estiver em execução, as alterações serão aplicadas somente após o aplicativo se iniciado localmente ou usando o Kaspersky Security Center.

Ativar proteção

Esta caixa de seleção ativa/desativa a proteção de um computador remoto com o Kaspersky Endpoint Security instalado.

Se essa caixa de seleção estiver marcada, a proteção do computador remoto estará ativada.

Se essa caixa de seleção estiver desmarcada, a proteção do computador remoto estará desativada.

Esta caixa de seleção está marcada por padrão.

Na seção **Tipos de objetos a serem detectados**, é possível selecionar os tipos de objetos que serão detectados pelo Kaspersky Endpoint Security.

Vírus, worms, trojans, ferramentas maliciosas, adwares e discadores automáticos

Esta caixa de seleção ativa/desativa a detecção dos seguintes tipos de programas:

- Todos os tipos de malware.
- Aplicativos que mostram anúncios (como banners) no seu computador ou que substituem os resultados de pesquisa no navegador por sites de publicidade.
- Aplicativos que secretamente estabelecem conexões telefônicas através do modem de um computador.

A caixa de seleção está marcada por padrão e não pode ser desmarcada.

Softwares legítimos que podem ser usados por intrusos para danificar seu computador ou dados pessoais

Essa caixa de seleção ativa/desativa a detecção de aplicativos que não sejam maliciosos ou perigosos, mas que, em determinadas circunstâncias, podem ser usados para danificar o computador do usuário.

Se a caixa de seleção estiver marcada, o Kaspersky Endpoint Security detectará o softwares legítimos que podem ser usados por intrusos para danificar o computador ou dados pessoais de um usuário.

Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não detectará softwares legítimos que podem ser usados por intrusos para danificar o computador ou dados pessoais de um usuário.

Esta caixa de seleção está desmarcada por padrão.

A seção **Avançado** permite ativar o modo de economia de energia.

Ignorar tarefas programadas quando a bateria estiver baixa

Esta caixa de seleção ativa/desativa o início das tarefas de verificação agendadas em computadores no modo de bateria.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security não iniciará as tarefas de verificação agendadas em computadores no modo de bateria.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security iniciará as tarefas de verificação agendadas em computadores no modo de bateria.

Esta caixa de seleção está marcada por padrão.

Limitar o uso de CPU pelas tarefas de verificação

O Kaspersky Endpoint Security limita o uso da CPU do dispositivo protegido para tarefas de verificação sob demanda ao valor especificado no campo de entrada correspondente.

A ativação dessa opção pode afetar negativamente o desempenho do Kaspersky Endpoint Security.

Essa opção é desativada por padrão.

Limite superior (em porcentagens)

Valor máximo permitido de uso da CPU para tarefas de verificação pelo Kaspersky Endpoint Security.

O campo de entrada estará disponível se a opção **Limitar o uso de CPU pelas tarefas de verificação** estiver selecionada.

Observação: O limite é acumulativo de todos os núcleos da CPU. O uso da CPU exibido no Monitor de Atividade é a soma do uso de cada núcleo da CPU e pode ficar acima de 100%.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela Relatórios e Backup

Na seção **Relatórios**, é possível definir as configurações para gerar e armazenar relatórios sobre eventos que ocorrerem durante a execução do Kaspersky Endpoint Security.

Excluir relatórios depois de dias

Esta caixa de seleção ativa/desativa a exclusão de relatórios após o período especificado.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security excluirá os relatórios após o período especificado. Por padrão, o Kaspersky Endpoint Security armazena os relatórios por 30 dias.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security armazenará os relatórios indefinidamente.

Esta caixa de seleção está marcada por padrão.

Registrar eventos não críticos

Esta caixa de seleção ativa/desativa o registro de eventos não críticos (como eventos informativos) no relatório. Os eventos não críticos não afetam a segurança.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security registrará os eventos informativos no relatório.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não registrará os eventos informativos no relatório.

Esta caixa de seleção está desmarcada por padrão.

Manter apenas eventos recentes

Esta caixa de seleção ativa/desativa a opção para manter somente as informações sobre os eventos importantes da execução anterior da tarefa.

Se essa caixa de seleção estiver marcada, sempre que uma tarefa for iniciada, o Kaspersky Endpoint Security removerá as informações sobre os eventos não críticos da execução anterior da tarefa, mas manterá as importantes (por exemplo, sobre um malware detectado) no relatório.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security manterá todas as informações da execução anterior da tarefa.

Esta caixa de seleção está desmarcada por padrão.

Na seção **Backup**, é possível especificar por quanto tempo os objetos podem ser armazenados no Backup.

Excluir objetos depois de dias

Esta caixa de seleção ativa/desativa a remoção de objetos do Backup após o período especificado.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security removerá os objetos do Backup após o período especificado. O período de armazenamento padrão é de 30 dias.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security armazenará os objetos no Backup indefinidamente.

Esta caixa de seleção está marcada por padrão.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela Interação do usuário

Na seção **Interface do aplicativo**, é possível configurar se o ícone do aplicativo será exibido na barra de menus em um computador remoto, e se um usuário poderá abrir a janela principal do Kaspersky Endpoint Security e usar a interface do aplicativo.

Exibir ícone de aplicativo na barra de menus

Esta caixa de seleção ativa/desativa a exibição do ícone do aplicativo na barra de menus em um computador remoto.

Se essa caixa de seleção estiver marcada, o ícone do aplicativo será exibido na barra de menus.

Se essa caixa de seleção estiver desmarcada, o ícone do aplicativo ficará oculto na barra de menus.

Esta caixa de seleção está marcada por padrão.

Permitir que o usuário abra o aplicativo

Esta caixa de seleção ativa/desativa a capacidade do usuário de abrir a janela principal do Kaspersky Endpoint Security e usar a interface do aplicativo em um computador remoto.

Se essa caixa de seleção estiver marcada, o usuário poderá abrir a janela principal do Kaspersky Endpoint Security e usar a interface do aplicativo em um computador remoto.

Se essa caixa estiver desmarcada, o Kaspersky Endpoint Security não permite que o usuário abra a janela principal do aplicativo e oculta a interface do aplicativo em um computador remoto.

Esta caixa de seleção está marcada por padrão.

Na seção **Notificações**, é possível ativar as notificações sobre os eventos do Kaspersky Endpoint Security e escolher o tipo preferido de notificação.

Notificações

O botão **Notificações** ativa/desativa as notificações sobre os eventos do Kaspersky Endpoint Security.

Se o botão **Notificações** estiver ligado, o Kaspersky Endpoint Security mostrará as notificações sobre os eventos que ocorrerem durante a execução de seus componentes.

Se o botão **Notificações** estiver desligado, o Kaspersky Endpoint Security não mostrará as notificações sobre os eventos que ocorrerem durante a execução de seus componentes.

Por padrão, esse botão está ativado.

Notificações do usuário

Clicar nesse link abre uma janela na qual é possível selecionar os tipos de notificações a serem usados para todos os tipos de eventos.

Na seção **Permitir que o usuário saia do aplicativo**, você pode configurar se o Kaspersky Endpoint Security pode ser desligado por um usuário em um computador remoto.

Exibir Sair no menu de contexto do ícone do aplicativo

Esta caixa de seleção ativa/desativa a disponibilidade do item **Sair** no menu de contexto do ícone do aplicativo, exibido na barra de menus.

Se essa caixa de seleção estiver marcada, o item **Sair** estará disponível no menu de contexto do ícone do aplicativo. O usuário pode sair do Kaspersky Endpoint Security no computador remoto.

Se essa caixa de seleção estiver desmarcada, o item **Sair** ficará indisponível no menu de contexto do ícone do aplicativo. O usuário não pode sair do Kaspersky Endpoint Security no computador remoto.

Esta caixa de seleção está marcada por padrão.

Na seção **Eventos no Kaspersky Security Center**, é possível selecionar o idioma de exibição dos eventos do Kaspersky Endpoint Security no Kaspersky Security Center.

Idioma de exibição

Nesta lista suspensa, você pode selecionar o idioma de exibição dos eventos do Kaspersky Endpoint Security no Kaspersky Security Center.

Na seção **Restrições**, é possível permitir o gerenciamento local das chaves e atualizações do Kaspersky Endpoint Security em um computador remoto.

Permitir que o usuário gerencie atualizações localmente

Esta caixa de seleção ativa/desativa o gerenciamento local das atualizações do Kaspersky Endpoint Security em um computador remoto.

Se essa caixa de seleção estiver marcada, o gerenciamento local das atualizações do Kaspersky Endpoint Security em um computador remoto será ativado.

Se essa caixa de seleção estiver desmarcada, as atualizações do Kaspersky Endpoint Security em um computador remoto poderão ser gerenciadas apenas usando o plugin de administração do Kaspersky Endpoint Security no Kaspersky Security Center.

Esta caixa de seleção está marcada por padrão.

Permitir que o usuário gerencie chaves localmente

Esta caixa de seleção ativa/desativa o gerenciamento local das chaves do Kaspersky Endpoint Security em um computador remoto.

Se a caixa de seleção estiver marcada, o gerenciamento local das chaves do Kaspersky Endpoint Security em um computador remoto será ativado.

Se a caixa de seleção estiver desmarcada, as chaves do Kaspersky Endpoint Security em um computador remoto poderão ser gerenciadas apenas usando o plugin de administração do Kaspersky Endpoint Security no Kaspersky Security Center.

Esta caixa de seleção está marcada por padrão.

Na seção **Proteção por senha**, você pode definir e configurar a senha para limitar ações indesejadas nos dispositivos do usuário.

Proteção por senha

O botão de alternância **Proteção por senha** ativa/desativa a proteção por senha de ações indesejadas nos dispositivos do usuários.

Se o botão de alternância **Proteção por senha** estiver ativado, você poderá definir e configurar uma senha para limitar as ações do usuário em seus dispositivos.

Se o botão de alternância **Proteção por senha** estiver desativado, um usuário poderá executar uma ação indesejada sem inserir uma senha.

Por padrão, esse botão está desativado.

Ativar esse botão de alternância abre uma janela na qual é possível configurar a senha para limitar ações indesejadas nos dispositivos dos usuários.

Configurações

Clicar nesse botão abre uma janela na qual é possível configurar a senha para limitar ações indesejadas nos dispositivos dos usuários.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela Notificações do usuário

Eventos

Esta coluna lista os eventos que podem ocorrer enquanto o Kaspersky Endpoint Security está em execução:

- **Eventos críticos**. Eventos de extrema importância em termos de segurança.
- **Falha funcional**. Eventos que causam falha no sistema.
- **Eventos importantes**. Eventos que o usuário deve observar.
- **Eventos informativos**. Eventos de natureza informativa.

Notificações

Uma notificação é uma mensagem pop-up que avisa o usuário sobre um evento.

A caixa de seleção na coluna **Notificações** ativa/desativa as notificações pop-up sobre os eventos de uma categoria específica.

Som

Uma notificação sonora associada a um evento.

A caixa de seleção na coluna **Som** ativa/desativa as notificações sonoras para eventos de uma categoria específica.

A janela “Zona Confiável”: a seção “Arquivos e pastas”

Adicionar

Clicar nesse botão abre uma caixa de diálogo na qual é possível adicionar um arquivo ou pasta à Zona Confiável.

Excluir

Clicar nesse botão remove o arquivo ou pasta selecionada da lista de exclusões.

Esse botão ficará disponível se a caixa de seleção ao lado do arquivo ou pasta estiver marcada.

Arquivo ou pasta

Essa coluna contém arquivos ou pastas adicionadas à Zona confiável.

Status

O botão nessa coluna ativa/desativa a verificação do arquivo ou pasta adicionada à Zona Confiável.

Se o botão estiver ativado, o Kaspersky Endpoint Security não verificará o arquivo ou pasta correspondente.

Se o botão estiver desativado, o Kaspersky Endpoint Security verificará o arquivo ou pasta correspondente.

Comentário

Informações sobre o arquivo ou pasta adicionada à Zona Confiável.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A caixa de diálogo “Adicionar exclusão”

Campo de entrada Insira um nome de arquivo, nome de pasta ou máscara

Caminho para um arquivo ou uma pasta, ou uma máscara de arquivos/pastas que será excluída do escopo de proteção.

Incluir subpastas

Esta caixa de seleção ativa/desativa a verificação de subpastas na pasta especificada no campo **Insira um nome de arquivo, nome de pasta ou máscara**.

Se esta caixa de seleção estiver marcada, o Kaspersky Endpoint Security não verificará as subpastas da pasta especificada durante as verificações de malware.

Caso essa caixa de seleção esteja desmarcada, durante as verificações de malware, o Kaspersky Endpoint Security apenas excluirá diretamente os arquivos da pasta especificada no campo **Insira um nome de arquivo, nome de pasta ou máscara**. As subpastas da pasta especificada são verificadas.

Esta caixa de seleção está marcada por padrão.

Na seção **Componentes**, é possível selecionar componentes que não verificarão o arquivo ou a pasta especificados.

Qualquer

O componente de Verificação ou de Proteção Contra Ameaças ao Arquivo não verificará o arquivo ou pasta especificada.

Da lista

Essa opção permite selecionar os componentes.

Proteção Contra Ameaças ao Arquivo

Se essa caixa de seleção estiver marcada, o componente de Proteção Contra Ameaças ao Arquivo não verificará o arquivo ou pasta especificada.

Essa caixa de seleção ficará disponível se a opção **Da lista** estiver marcada.

Verificação

Se essa caixa de seleção estiver marcada, o componente de Verificação não verificará o arquivo ou pasta especificada.

Essa caixa de seleção ficará disponível se a opção **Da lista** estiver marcada.

Campo de entrada Comentário

Informações sobre o arquivo ou pasta adicionada à Zona Confiável.

Na seção **Status**, é possível selecionar se a exclusão está ou não ativa.

Desativado

O Kaspersky Endpoint Security verifica o arquivo ou pasta correspondente.

Ativado

O Kaspersky Endpoint Security não verifica o arquivo ou pasta correspondente.

A janela “Zona Confiável”: a seção “Aplicativos confiáveis”

Lista de aplicativos confiáveis

A lista de aplicativos confiáveis cujas atividades de rede não serão monitoradas pelo Kaspersky Endpoint Security.

Adicionar

Clicar nesse botão abre uma caixa de diálogo na qual é possível inserir um caminho para um aplicativo cujas atividades de rede não serão monitoradas pelo Kaspersky Endpoint Security.

Excluir

Clicar nesse botão remove o aplicativo confiável selecionado da lista.

Esse botão ficará disponível se a caixa de seleção ao lado do aplicativo confiável estiver marcada.

Aplicativo

Essa coluna contém o nome do aplicativo ou o último segmento do caminho para um aplicativo.

Status

Essa coluna contém um botão que indica o status de monitoramento da atividade de rede do aplicativo.

Se o status for **Ativado**, a atividade de rede do aplicativo correspondente não será monitorada pelo Kaspersky Endpoint Security.

Se o status for **Desativado**, a atividade de rede do aplicativo correspondente será monitorada pelo Kaspersky Endpoint Security.

Caminho

Essa coluna contém o caminho do aplicativo no computador cliente, adicionado manualmente.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A caixa de diálogo “Adicionar aplicativo”

Campo de entrada Caminho

O caminho para um aplicativo cujas atividades de rede ou de arquivos não serão monitoradas pelo aplicativo Kaspersky Endpoint Security.

Requisito de assinatura de código

Requisitos para a assinatura do código do aplicativo cuja atividade não será monitorada pelo Kaspersky Endpoint Security.

Este é um parâmetro opcional.

Opções

Nesta seção, você pode selecionar os tipos de atividades que não deseja que sejam monitoradas pelo aplicativo Kaspersky Endpoint Security.

Não monitorar a atividade de arquivos

Esta caixa de seleção ativa/desativa o monitoramento das operações de um aplicativo com arquivos em um computador cliente.

Se esta caixa de seleção estiver marcada, o Kaspersky Endpoint Security não monitorará a atividade de arquivos do aplicativo.

Se esta caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security monitorará a atividade de arquivos do aplicativo.

Esta caixa de seleção está marcada por padrão.

Não monitorar a atividade de rede

Esta caixa de seleção ativa/desativa o monitoramento do tráfego de entrada e saída da Internet do aplicativo em um computador cliente.

Se a caixa de seleção estiver marcada, o Kaspersky Endpoint Security não monitorará a atividade de rede do aplicativo.

Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security monitorará a atividade de rede do aplicativo.

Esta caixa de seleção está marcada por padrão.

A janela Rede

Na seção **Configurações do servidor proxy**, você pode definir o uso de um servidor proxy e as configurações a serem usadas para conectar-se a um servidor proxy.

Não usar servidor proxy

Se esta opção estiver selecionada, o Kaspersky Endpoint Security não usará um servidor proxy para conectar-se a fontes de atualização de bancos de dados e módulos do aplicativo.

Usar configurações de servidor proxy do sistema

Se esta opção estiver selecionada, o Kaspersky Endpoint Security se conectará a fontes de atualização de bancos de dados e módulos do aplicativo usando as configurações do servidor proxy definidas no seu sistema operacional.

Esta opção está marcada por padrão.

Usar configurações de servidor proxy especificadas

Se esta opção estiver selecionada, o Kaspersky Endpoint Security se conectará a fontes de atualização de bancos de dados e módulos do aplicativo usando as configurações do servidor proxy que você especificou.

Endereço

Endereço IP ou nome simbólico de um servidor proxy.

Este campo ficará disponível se a opção **Usar configurações de servidor proxy especificadas** for marcada.

Porta

Número da porta do servidor proxy.

O número da porta padrão é 8080.

Este campo ficará disponível se a opção **Usar configurações de servidor proxy especificadas** for marcada.

Usar autenticação

Esta caixa de seleção ativa/desativa o uso da autenticação ao conectar-se a um servidor proxy.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security exigirá as credenciais do usuário para se conectar a um servidor proxy.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não exigirá as credenciais do usuário para se conectar a um servidor proxy.

Esta caixa de seleção está marcada por padrão.

Essa caixa de seleção ficará disponível se a opção **Usar configurações de servidor proxy especificadas** for marcada.

Nome do usuário

Nome de usuário para conectar-se ao servidor proxy.

Este campo ficará disponível se a opção **Usar configurações de servidor proxy especificadas** e a caixa de seleção **Usar autenticação** forem marcadas.

Senha

Senha para o nome de usuário especificado.

Este campo ficará disponível se a opção **Usar configurações de servidor proxy especificadas** e a caixa de seleção **Usar autenticação** forem marcadas.

Exibir

Ao clicar neste botão, os caracteres da senha digitada serão exibidos no campo **Senha**.

Ignorar servidor proxy para endereços locais

Esta caixa de seleção ativa/desativa o uso de um servidor proxy ao atualizar bancos de dados e módulos do aplicativo de uma pasta local ou de rede.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security não usará um servidor proxy ao atualizar bancos de dados e módulos do aplicativo de uma pasta local ou de rede.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security usará um servidor proxy ao atualizar bancos de dados e módulos do aplicativo de uma pasta local ou de rede.

Esta caixa de seleção está marcada por padrão.

Essa caixa de seleção ficará disponível se a opção **Usar configurações de servidor proxy especificadas** for marcada.

Na seção **Verificar conexões seguras**, é possível definir se o Kaspersky Endpoint Security verificará as conexões seguras (HTTPS).

Verificação de conexões seguras (HTTPS)

O botão **Verificação de conexões seguras (HTTPS)** ativa/desativa a verificação de conexões seguras estabelecidas pelo protocolo HTTPS e a exibição de notificações quando o Controle da Web bloqueia o acesso do usuário a recursos da Web perigosos.

Se o botão **Verificação de conexões seguras (HTTPS)** estiver ativado, o Kaspersky Endpoint Security fará o seguinte:

- A Proteção Contra Ameaças da Web verificará os dados enviados e recebidos pelo seu computador por meio do protocolo HTTPS no Safari, Google Chrome ou Firefox.
- O aplicativo exibirá as notificações quando o usuário acessar os recursos da Web bloqueados pelo Controle da Web no computador remoto.

Se o botão **Verificação de conexões seguras (HTTPS)** estiver desativado, o Kaspersky Endpoint Security fará o seguinte:

- A Proteção Contra Ameaças da Web não verificará os dados enviados e recebidos pelo seu computador por meio do protocolo HTTPS.
- O aplicativo não exibirá as notificações quando o usuário acessar os recursos da Web bloqueados pelo Controle da Web no computador remoto.

Por padrão, esse botão está ativado.

Na seção **Selecione o armazenamento de certificados a ser usado pelo Firefox**, você pode selecionar o armazenamento de certificados para verificar o tráfego HTTPS criptografado no navegador Mozilla Firefox.

Chave Raízes do Sistema (recomendado)

Se essa opção estiver selecionada, o Kaspersky Endpoint Security usará um certificado raiz da chave Raízes do Sistema para verificar o tráfego HTTPS criptografado no navegador Mozilla Firefox.

Esta opção está marcada por padrão.

Armazenamento de certificados nos ajustes do navegador Mozilla Firefox

Se essa opção estiver selecionada, o Kaspersky Endpoint Security usará o certificado do armazenamento de certificados do navegador.

Nesse caso, será necessário adicionar manualmente o certificado do Kaspersky Endpoint Security ao armazenamento de certificados do navegador Mozilla Firefox. Para obter mais informações, consulte Como adicionar o certificado da Kaspersky ao armazenamento de certificados do Mozilla Firefox.

Na seção **Certificados raiz confiáveis**, é possível gerenciar a lista de certificados raiz confiáveis.

Gerenciar certificados raiz confiáveis

Clicar nesse link abre uma janela na qual é possível criar uma lista de certificados raiz confiáveis para se conectar ao servidores sem notificações.

Na seção **Portas monitoradas**, é possível configurar quais portas são monitoradas pelo Kaspersky Endpoint Security.

Portas selecionadas

Clicar nesse link abre uma janela na qual é possível configurar uma lista de portas que são monitoradas pelo Kaspersky Endpoint Security.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela “Gerenciar certificados raiz confiáveis”

Adicionar

Clicar nesse botão abre um diálogo para adicionar certificados que serão considerados confiáveis.

Excluir

Clicar neste botão remove o certificado selecionado da lista.

Lista de certificados confiáveis

Uma lista exibindo os nomes dos certificados raiz confiáveis.

Por padrão, a lista está vazia.

Aplicar

Quando o botão **Aplicar** estiver ligado, o Kaspersky Endpoint Security proibirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

Quando o botão **Aplicar** estiver desligado, o Kaspersky Endpoint Security permitirá a alteração de valores das configurações de tarefas, das configurações de aplicativos, de políticas de subgrupos e de Servidores de Administração secundários em um computador local.

A janela Portas monitoradas

Lista de portas monitoradas

Uma lista de portas para as quais é possível configurar o monitoramento de dados transmitidos.

Por padrão, a lista contém as portas usadas com frequência pelos serviços mais comuns.

Adicionar

Clicar nesse botão abre uma caixa de diálogo na qual é possível adicionar uma porta para ser monitorada pelo Kaspersky Endpoint Security.

Excluir

Clicar nesse botão remove a porta selecionada da lista.

Esse botão ficará disponível se a caixa de seleção ao lado da porta estiver marcada.

Porta

Essa coluna contém os números de porta.

Status

Essa coluna contém um botão que indica o status de monitoramento dos dados transmitidos pela porta.

Se o status for **Monitoradas**, o tráfego transmitido pela porta correspondente será verificado pelo Kaspersky Endpoint Security.

Se o status for **Não monitoradas**, o tráfego transmitido pela porta correspondente não será verificado pelo Kaspersky Endpoint Security.

Descrição

Essa coluna contém uma descrição da porta.

A caixa de diálogo “Adicionar porta”

Campo de entrada Porta

O número de uma porta para a qual você deseja que o Kaspersky Endpoint Security verifique os dados transmitidos.

Campo de entrada Descrição

Informações adicionais sobre a porta; por exemplo, o tipo de porta.

A janela “Informações sobre a licença”

Na janela **Informações sobre a licença**, é possível visualizar as informações sobre uma licença, incluindo sua data de expiração, o número de computadores nos quais é possível usar o Kaspersky Endpoint Security com essa licença e o tipo de licença.

Adicionar uma chave reserva

Esta caixa de seleção ativa/desativa a adição de um arquivo de chave ou código de ativação específico como uma chave reserva.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security adicionará o arquivo de chave ou o código de ativação especificado como uma chave reserva.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security adicionará o arquivo de chave ou o código de ativação especificado como a chave ativa.

Esta caixa de seleção está desmarcada por padrão.

A janela “Verificação”

Escopo da verificação

Clicar nesse link abre uma janela na qual é possível criar o escopo da verificação.

Na seção **Se um objeto malicioso for detectado**, é possível selecionar a ação que o Kaspersky Endpoint Security deve executar ao detectar um objeto infectado.

Solicitar ação do usuário após verificação

O Kaspersky Endpoint Security não processa objetos até que a verificação seja concluída. Nesse momento, o Kaspersky Endpoint Security exibe uma notificação com informações sobre cada objeto infectado e solicita que o usuário selecione qual ação executar. As opções disponíveis dependem do tipo de objeto.

Esta opção está marcada por padrão.

Solicitar ação imediata do usuário

O Kaspersky Endpoint Security exibe uma notificação com informações sobre cada objeto infectado que o aplicativo detecta e solicita que o usuário selecione uma ação adicional. As opções disponíveis dependem do tipo de objeto.

Não solicitar ação

O Kaspersky Endpoint Security registra as informações sobre os objetos detectados no relatório sem processá-los.

Desinfectar automaticamente

Esta caixa de seleção ativa/desativa a desinfecção de objetos infectados detectados pelo Kaspersky Endpoint Security sem solicitar a confirmação ao usuário.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security desinfectará automaticamente os objetos infectados.

Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security ignorará os objetos infectados.

Essa caixa de seleção ficará disponível se a opção **Não solicitar ação** for marcada.

Esta caixa de seleção está marcada por padrão.

Desinfectar, excluir se a desinfecção falhar

Esta caixa de seleção ativa/desativa a remoção de objetos infectados ou provavelmente infectados após uma falha ao desinfectá-los.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security removerá automaticamente os objetos infectados que não puderam ser desinfectados.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não removerá os objetos infectados que não puderam ser desinfectados.

Esta caixa de seleção será exibida se a opção **Não solicitar ação** e a caixa de seleção **Desinfectar automaticamente** estiverem marcadas.

Esta caixa de seleção está marcada por padrão.

Na seção **Tipos de arquivos**, é possível selecionar o formato dos arquivos a serem verificados pelo Kaspersky Endpoint Security.

Verificar todos os arquivos

O Kaspersky Endpoint Security verifica todos os objetos do sistema de arquivos que são executados, abertos ou salvos.

Verificar aplicativos e documentos por conteúdo

O Kaspersky Endpoint Security verifica somente os objetos que podem estar infectados com base no formato do arquivo.

A lista de formatos de arquivos é definida pela Kaspersky e faz parte dos bancos de dados do Kaspersky Endpoint Security.

Verificar aplicativos e documentos por extensão

O Kaspersky Endpoint Security verifica somente os objetos que podem estar infectados com base na extensão do arquivo.

A lista de extensões de arquivos é definida pela Kaspersky e faz parte dos bancos de dados do Kaspersky Endpoint Security.

O Kaspersky Endpoint Security sempre verifica os arquivos sem extensões.

Na seção **Otimização**, é possível configurar o desempenho da verificação.

Verificar apenas arquivos novos e modificados

Essa caixa de seleção ativa/desativa a verificação apenas dos arquivos que o Kaspersky Endpoint Security reconhece como novos ou modificados desde a verificação anterior.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará apenas os arquivos que reconhecer como novos ou modificados desde a última verificação.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará todos os arquivos.

Ignorar a verificação de volumes de sistema somente leitura

Esta caixa de seleção ativa/desativa a verificação do volume do sistema somente leitura pelo Kaspersky Endpoint Security.

Caso esta caixa de seleção esteja marcada, o Kaspersky Endpoint Security não verificará o volume do sistema em somente leitura. Isso reduz significativamente o tempo de verificação.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará o volume do sistema somente leitura.

Esta caixa de seleção está marcada por padrão.

Ignorar arquivos maiores que MB

Esta caixa de seleção ativa/desativa a exclusão de arquivos maiores que o tamanho especificado da verificação.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security ignorará os arquivos maiores que o tamanho especificado.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará os arquivos, independentemente do tamanho.

Esta caixa de seleção está desmarcada por padrão.

Por padrão, o tamanho é definido como 100 MB.

Ignorar se a verificação demorar mais do que s

Esta caixa de seleção ativa/desativa o limite de duração das verificações de arquivo. O Kaspersky Endpoint Security ignorará um arquivo se a verificação dele exceder o limite de tempo especificado.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security ignorará um arquivo se a verificação dele exceder o limite de tempo especificado.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará os arquivos, independentemente de quanto tempo a verificação possa demorar.

O valor padrão é 30 segundos.

Na seção **Arquivos compostos**, é possível selecionar os tipos de arquivos compostos verificados pelo Kaspersky Endpoint Security.

Verificar arquivos comprimidos

Esta caixa de seleção ativa/desativa a verificação de arquivos.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará os arquivos.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security ignorará os arquivos durante as verificações.

Todos

O Kaspersky Endpoint Security verificará todos os arquivos.

Essa opção ficará disponível se a caixa de seleção **Verificar arquivos comprimidos** estiver marcada.

Apenas novos

O Kaspersky Endpoint Security verificará apenas novos arquivos comprimidos.

Essa opção ficará disponível se a caixa de seleção **Verificar arquivos comprimidos** estiver marcada.

Verificar arquivos comprimidos protegidos por senha

Esta caixa de seleção ativa/desativa a verificação de arquivos protegidos por senha.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará os arquivos protegidos por senha.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security ignorará os arquivos protegidos por senha durante a verificação.

Verificar objetos OLE incorporados

Esta caixa de seleção ativa/desativa a verificação de objetos incorporados em um arquivo, como planilhas do Excel, macros ou anexos de e-mail.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará os objetos OLE incorporados.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security ignorará os objetos OLE incorporados durante as verificações.

Todos

O Kaspersky Endpoint Security verificará todos os objetos OLE.

Essa opção ficará disponível se a caixa de seleção **Verificar objetos OLE incorporados** estiver marcada.

Apenas novos

O Kaspersky Endpoint Security verificará apenas novos objetos OLE incorporados.

Essa opção ficará disponível se a caixa de seleção **Verificar objetos OLE incorporados** estiver marcada.

Verificar arquivos de formato de e-mail

Esta caixa de seleção ativa/desativa a verificação de arquivos em formatos e bancos de dados de e-mail.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará os arquivos nos formatos e bancos de dados de e-mail.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security ignorará os arquivos nos formatos e bancos de dados de e-mail durante as verificações.

Janela Escopo de verificação

Adicionar

Clicar nesse botão abre uma caixa de diálogo na qual é possível especificar um arquivo, uma pasta ou uma máscara de arquivo/pasta a ser adicionada ao escopo da verificação.

Excluir

Clicar no botão remove um objeto do escopo da verificação.

Esse botão ficará disponível se a caixa de seleção ao lado do objeto estiver marcada.

Não é possível excluir os objetos padrão incluídos no escopo da verificação.

Escopo da verificação

Essa coluna contém os objetos verificados durante uma verificação de malware.

Status

O botão nesta coluna ativa/desativa a verificação dos objetos adicionados ao escopo da verificação.

Se o botão estiver ativado, o Kaspersky Endpoint Security verificará o objeto correspondente.

Se o botão estiver desativado, o Kaspersky Endpoint Security não verificará o objeto correspondente.

Adicional

Essa coluna indica se o Kaspersky Endpoint Security verificará as subpastas do objeto correspondente.

Nota: o Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.

A caixa de diálogo “Adicionar escopo da verificação”

Insira um nome de arquivo, nome de pasta ou máscara

Caminho para um arquivo, uma pasta ou uma máscara de arquivos/ pastas.

O objeto é uma pasta

Esta caixa de seleção ativa/desativa a verificação de um objeto como uma pasta.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará o objeto especificado no campo **Insira um nome de arquivo, nome de pasta ou máscara** como uma pasta.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará o objeto especificado no campo **Insira um nome de arquivo, nome de pasta ou máscara** como um arquivo.

Esta caixa de seleção está marcada por padrão.

Incluir subpastas

Esta caixa de seleção ativa/desativa a verificação de subpastas na pasta especificada no campo **Insira um nome de arquivo, nome de pasta ou máscara**.

Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security verificará as subpastas durante as verificações de malware.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará apenas os arquivos diretamente na pasta especificada no campo **Insira um nome de arquivo, nome de pasta ou máscara** durante as verificações de malware.

Esta caixa de seleção está marcada por padrão.

Nota: o Kaspersky Endpoint Security não verifica arquivos localizados no armazenamento do OneDrive ou do iCloud ou em outros armazenamentos na nuvem. Exclua esses arquivos do escopo da verificação. Caso contrário, a tarefa de verificação poderá ser concluída com o erro *Arquivo infectado não excluído*.

A janela Parâmetros do arquivo

Os seguintes tipos de hashes de arquivo são compatíveis:

- **MD5**

  Um hash desse tipo deve ter 32 caracteres e conter 0-9, a-f, A-F.

- **SHA256**

  Um hash desse tipo deve ter 64 caracteres e conter 0-9, a-f, A-F.