Kaspersky Embedded Systems Security

Manual do Administrador

Versão do aplicativo: 2.2.0.605

Prezado usuário,

Obrigado por escolher a Kaspersky Lab como seu provedor de software de segurança. Esperamos que este documento o ajude a usar o nosso produto.

Data de revisão do documento: 07.12.2018

https://www.kaspersky.com.br/
https://support.kaspersky.com.br/

Conteúdo

Sobre este Manual

O Manual do Usuário do Kaspersky Embedded Systems Security 2.2.0.605 (doravante referido como “Kaspersky Embedded Systems Security 2.2”, “o aplicativo”) é destinado a especialistas que instalam e administram o Kaspersky Embedded Systems Security 2.2 em todos os dispositivos protegidos e aos que fornecem suporte técnico a organizações que usam o Kaspersky Embedded Systems Security 2.2.

Este Manual contém informações sobre como configurar e usar o Kaspersky Embedded Systems Security 2.2.

Ele também fornecerá fontes de informação sobre o aplicativo e formas de receber suporte técnico.

Neste capítulo

Nesta documentação

O Manual do Administrador do Kaspersky Embedded Systems Security 2.2 contém as seguintes seções:

Fontes de informação sobre o Kaspersky Embedded Systems Security 2.2

Esta seção lista as fontes de informação sobre o aplicativo.

Kaspersky Embedded Systems Security 2.2

Esta seção descreve as funções, os componentes e o kit de distribuição do Kaspersky Embedded Systems Security 2.2, e fornece uma lista dos requisitos de hardware e software do Kaspersky Embedded Systems Security 2.2.

Instalação e remoção do aplicativo

Esta seção fornece instruções passo a passo para instalar e remover o Kaspersky Embedded Systems Security 2.2.

Interface do aplicativo

Esta seção contém informações sobre os elementos da interface do Kaspersky Embedded Systems Security 2.2:

Licenciamento do aplicativo

Esta seção fornece informações sobre os principais conceitos relacionados ao licenciamento do aplicativo.

Inicialização e interrupção do Kaspersky Embedded Systems Security 2.2

Esta seção contém informações sobre como inicializar e interromper o Plug-in de Administração do Kaspersky Embedded Systems Security 2.2 (doravante referido como Plug-in de Administração) e o Kaspersky Security Service.

Sobre permissões de acesso para funções do Kaspersky Embedded Systems Security 2.2

Esta seção contém informações sobre permissões para gerenciar o Kaspersky Embedded Systems Security 2.2 e os serviços Windows® registrados pelo aplicativo, bem como instruções sobre como configurar essas permissões.

Criando e configurando políticas

Esta seção contém informações sobre como utilizar as políticas do Kaspersky Security Center para gerenciar o Kaspersky Embedded Systems Security 2.2 em vários computadores.

Criando e configurando uma tarefa usando o Kaspersky Security Center

Esta seção contém informação sobre tarefas do Kaspersky Embedded Systems Security 2.2 e como criá-las, definir suas configurações, iniciá-las e interrompê-las.

Gerenciamento das configurações do aplicativo

Esta seção contém informações sobre como definir as configurações gerais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center.

Proteção do Computador em Tempo Real

Esta seção fornece informações sobre as tarefas de Proteção do Computador em Tempo Real: Proteção de Arquivos em Tempo Real, Uso da KSN, além da funcionalidade de Prevenção de Exploits. Ela também fornece instruções sobre como configurar tarefas de Proteção em Tempo Real e gerenciar as configurações de segurança de um computador protegido.

Controle de Atividades Locais

Esta seção fornece informações sobre a funcionalidade do Kaspersky Embedded Systems Security 2.2 que controla inicializações de aplicativos, conexões de dispositivos externos via USB.

Controle de atividade de rede

Esta seção contém informações sobre a tarefa Gerenciamento de Firewall.

Inspeção do sistema

Esta seção contém informações sobre a tarefa Monitor de Integridade de Arquivos e recursos para inspecionar o log do sistema operacional.

Integração com sistemas de terceiros

Esta seção descreve a integração do Kaspersky Embedded Systems Security 2.2 com recursos e tecnologias de terceiros.

Trabalhando com o Kaspersky Embedded Systems Security 2.2 a partir da linha de comando

Esta seção descreve como trabalhar com o Kaspersky Embedded Systems Security 2.2 a partir da linha de comando.

Entrando em contato com o Suporte Técnico

Esta seção descreve as formas de receber suporte técnico e as condições em que ele está disponível.

Glossário

Esta seção contém uma lista dos termos mencionados no documento, bem como suas respetivas definições.

AO Kaspersky Lab

Esta seção fornece informações sobre a AO Kaspersky Lab.

Informações sobre código de terceiros

Esta seção contém informações sobre códigos de terceiros utilizados no aplicativo.

Notificações de marcas registradas

Esta seção lista marcas registradas reservadas a proprietários terceiros e mencionados no documento.

Índice

Esta seção permite encontrar rapidamente informações no documento.

Convenções da documentação

Este documento utiliza as seguintes convenções (consulte a tabela abaixo).

Tabela 1. Convenções da documentação

Texto de exemplo	Descrição das convenções da documentação
Observe que...	Os avisos são realçados em vermelho e exibidos em uma caixa. Os avisos contêm informações sobre as ações que podem ter consequências indesejáveis.
É recomendável usar...	As observações são exibidas em uma caixa. As observações contêm informações adicionais e de referência.
Exemplo: ...	Os exemplos são dados em blocos sobre fundo azul, sob o título "Exemplo".
Atualização significa... Ocorreu o evento Bancos de dados desatualizados.	Os seguintes elementos são exibidos no texto em itálico: • Termos novos • Nomes de status e eventos do aplicativo
Pressione ENTER. Pressione ALT+F4.	Os nomes de teclas do teclado são exibidos em negrito e em letras maiúsculas. Os nomes das teclas seguidos de um sinal de + (adição) indicam o uso de uma combinação de teclas. Estas teclas devem ser pressionadas simultaneamente.
Clique no botão **Ativar**.	Os nomes de elementos da interface do aplicativo, como caixas de texto, itens de menu e botões são exibidos em negrito.
► *Para configurar a programação da tarefa:*	As frases introdutórias de instruções são exibidas em itálico e acompanhadas de um sinal de seta.

Texto de exemplo	Descrição das convenções da documentação
Na linha de comandos, insira `help` Em seguida, a seguinte mensagem será exibida: Especifique a data no formato `dd:mm:aa`.	Os seguintes tipos de conteúdo de texto são exibidos com uma fonte especial: • Texto da linha de comando • O texto de mensagens exibido na tela pelo aplicativo • Dados que devem ser inseridos a partir do teclado
<Nome de usuário>	As variáveis são colocadas entre colchetes angulares. Em vez de uma variável, o valor correspondente deve ser inserido, sem os colchetes angulares.

Fontes de informação sobre o Kaspersky Embedded Systems Security 2.2

Esta seção lista as fontes de informação sobre o aplicativo.

Você pode selecionar a fonte de informações mais adequada de acordo com o nível de importância e a urgência do problema.

Neste capítulo

Fontes para a recuperação independente de informações

Você pode usar as fontes seguintes para encontrar informação sobre o Kaspersky Embedded Systems Security 2.2:

- Página do Kaspersky Embedded Systems Security 2.2 no site da Kaspersky Lab.
- A página do Kaspersky Embedded Systems Security 2.2 no site de Suporte Técnico (Base de Dados de Conhecimento).
- Manuais.

> Se você não encontrou uma solução para o seu problema, entre em contato com o Suporte Técnico da Kaspersky Lab https://support.kaspersky.com.br/.

> É requerida uma conexão da Internet para usar fontes de informação on-line.

Página do Kaspersky Embedded Systems Security 2.2 no site da Kaspersky Lab

Na página do Kaspersky Embedded Systems Security 2.2 (https://www.kaspersky.com.br/enterprise-security/embedded-systems), você pode visualizar informações gerais sobre o aplicativo, suas funções e recursos.

A página do Kaspersky Embedded Systems Security 2.2 contém um link para a Loja Virtual. Lá, você pode comprar o aplicativo ou renovar sua licença.

Página do Kaspersky Embedded Systems Security 2.2 na Base de Dados de Conhecimento

A Base de Dados de Conhecimento é uma seção do site de Suporte Técnico.

A página do Kaspersky Embedded Systems Security 2.2 na Base de Dados de Conhecimento (https://support.kaspersky.com/kess2/) inclui artigos que fornecem informações úteis, recomendações e respostas a perguntas frequentes sobre como comprar, instalar e usar o aplicativo.

Os artigos da Base de Dados de Conhecimento podem responder a perguntas relacionadas não só com o Kaspersky Embedded Systems Security 2.2, mas também com outros aplicativos da Kaspersky Lab. Os artigos da Base de Dados de Conhecimento podem também incluir notícias sobre o Suporte Técnico.

Documentação do Kaspersky Embedded Systems Security 2.2

O Manual do Administrador do Kaspersky Embedded Systems Security 2.2 contém informações sobre a instalação, desinstalação, definição das configurações e uso do aplicativo.

Discutindo os aplicativos do Kaspersky Lab no fórum da Web

Se a sua pergunta não precisar de uma resposta urgente, você poderá discuti-la com os especialistas da Kaspersky Lab e com outros usuários no nosso fórum http://forum.kaspersky.com/.

No fórum, é possível visualizar os threads existentes, deixar seus comentários e criar novos threads de discussão.

Kaspersky Embedded Systems Security 2.2

Esta seção descreve as funções, os componentes e o kit de distribuição do Kaspersky Embedded Systems Security 2.2, e fornece uma lista dos requisitos de hardware e software do Kaspersky Embedded Systems Security 2.2.

Neste capítulo

Sobre o Kaspersky Embedded Systems Security 2.2

O Kaspersky Embedded Systems Security 2.2 protege computadores e outros sistemas incorporados do Microsoft® Windows contra vírus e outras ameaças de computador. Os usuários do Kaspersky Embedded Systems Security 2.2 são administradores da rede corporativa e especialistas responsáveis pela proteção antivírus da rede corporativa.

Você pode instalar o Kaspersky Embedded Systems Security 2.2 em uma variedade de sistemas incorporados do Windows, incluindo os seguintes tipos de dispositivos:

- ATM (caixas eletrônicos);
- POS (pontos de vendas).

O Kaspersky Embedded Systems Security 2.2 pode ser gerenciado das seguintes formas:

- Por meio do Console do Aplicativo instalado no mesmo computador em que o Kaspersky Embedded Systems Security 2.2 está instalado, ou em um computador diferente.
- Usando comandos na linha de comandos.
- Por meio do Console de Administração do Kaspersky Security Center.

O aplicativo Kaspersky Security Center também pode ser usado para a administração centralizada de vários computadores executando o Kaspersky Embedded Systems Security 2.2.

É possível examinar os contadores de desempenho do Kaspersky Embedded Systems Security 2.2 para o aplicativo "Monitor do Sistema", além de contadores e interceptações SNMP.

Componentes e funções do Kaspersky Embedded Systems Security 2.2

O aplicativo inclui os seguintes componentes:

- **Proteção de Arquivos em Tempo Real**. O Kaspersky Embedded Systems Security 2.2 verifica objetos quando eles são acessados. O Kaspersky Embedded Systems Security 2.2 verifica os seguintes objetos:
  - Arquivos
  - Fluxos alternativos do sistema de arquivos (Fluxos NTFS)
  - Registro mestre de inicialização e setores de inicialização nos discos rígidos locais e unidades removíveis

- **Verificação por Demanda**. O Kaspersky Embedded Systems Security 2.2 executa uma única verificação da área especificada quanto à existência de vírus e outras ameaças à segurança do computador. O aplicativo verifica arquivos, RAM e objetos de inicialização em um computador protegido.
- **Controle de Inicialização de Aplicativos**. O componente rastreia todas as tentativas dos usuários de iniciar os aplicativos e controla as inicializações de aplicativos em um computador protegido.
- **Controle de Dispositivos**. O componente controla o registro e o uso de dispositivos de armazenamento em massa e unidades de CD/DVD para proteger o computador contra ameaças à segurança que possam surgir enquanto os arquivos são trocados com pen drives conectados por USB ou outros tipos de dispositivo externo.
- **Gerenciamento de Firewall**. Este componente fornece a capacidade de gerenciar o Firewall do Windows: definir configurações e regras de Firewall do sistema operacional e bloquear qualquer possibilidade de configuração externa do Firewall.
- **Monitor de Integridade de Arquivos**. O Kaspersky Embedded Systems Security 2.2 detecta mudanças nos arquivos dentro dos escopos de monitoramento especificados nas configurações da tarefa. Essas mudanças podem indicar uma violação de segurança no computador protegido.
- **Inspeção do Log**. Este componente monitora a integridade do ambiente protegido com base nos resultados de uma inspeção dos logs de evento do Windows.

As funções que se seguem são implementadas no aplicativo:

- **Atualização do Banco de Dados e Atualização dos Módulos de Software**. O Kaspersky Embedded Systems Security 2.2 baixa atualizações dos bancos de dados e módulos do aplicativo a partir de servidores de atualização FTP ou HTTP da Kaspersky Lab, do Servidor de Administração do Kaspersky Security Center ou de outras fontes de atualização.
- **Quarentena**. O Kaspersky Embedded Systems Security 2.2 coloca na Quarentena objetos possivelmente infectados movendo esses objetos da sua localização original para a *Quarentena*. Por questões de segurança, os objetos são armazenados na Quarentena em formato criptografado.
- **Backup**. O Kaspersky Embedded Systems Security 2.2 armazena cópias criptografadas de objetos classificados como *Infectados* ou *Possivelmente infectados* no *Backup* antes de desinfectá-los ou removê-los.
- **Notificações do administrador e do usuário**. Você pode configurar o aplicativo para notificar o administrador e os usuários que acessam o computador protegido sobre eventos na operação do Kaspersky Embedded Systems Security 2.2 e no status da proteção de antivírus no computador.
- **Configurações de importação e exportação**. Você pode exportar as configurações do Kaspersky Embedded Systems Security 2.2 para um arquivo de configuração XML e importar configurações para o Kaspersky Embedded Systems Security 2.2 a partir do arquivo de configuração. Em um arquivo de configuração, é possível salvar todas as configurações do aplicativo ou apenas aquelas para componentes individuais.
- **Aplicando modelos**. É possível definir manualmente as configurações de segurança de um nó na árvore ou em uma lista dos recursos de arquivos de computador e salvar os valores das configurações definidas como um modelo. Esse modelo pode então ser usado para definir as configurações de segurança de outros nós nas tarefas de proteção e de verificação do Kaspersky Embedded Systems Security 2.2.
- **Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security**. É possível configurar os direitos para gerenciar o Kaspersky Embedded Systems Security 2.2 e os serviços do Windows registrados pelo aplicativo, para usuários e grupos deles.
- **Gravação de eventos no log de eventos de aplicativo**. O Kaspersky Embedded Systems Security 2.2 registra informações sobre as configurações dos componentes de software, o status atual de tarefas, eventos que ocorreram durante a sua execução, eventos associados ao gerenciamento do Kaspersky

Embedded Systems Security 2.2 e informações necessárias para o diagnóstico de erros no Kaspersky Embedded Systems Security 2.2.

- **Zona Confiável**. Você pode gerar a lista de exclusões da proteção ou do escopo da verificação que o Kaspersky Embedded Systems Security 2.2 aplicará nas tarefas de proteção por demanda e em tempo real.
- **Prevenção de Exploits**. É possível proteger a memória do processo contra exploits usando um agente injetado no processo.

O que há de novo

O Kaspersky Embedded Systems Security 2.2 oferece os seguintes novos recursos e aprimoramentos:

- Suporte para novas versões de sistemas operacionais Microsoft Windows.

  Mecanismos de autodefesa baseados em tecnologias ELAM e PPL: agora, quando o aplicativo for instalado, ele registra automaticamente um driver ELAM que permite iniciar o Kaspersky Security Service (kavfs.exe) com o atributo de Processo protegido Superficial. Isto permite reforçar a autodefesa do aplicativo e prevenir uma ampla gama de ataques.

  A funcionalidade está disponível quando o aplicativo é instalado em computadores executando Microsoft Windows 10 RS2 (compilação número 15063) e posterior.
- Suporte para verificação e processamento de arquivos de nuvem armazenados no Microsoft OneDrive.
- As possibilidades de subsistema de controle de distribuição de software foram aprimoradas.

  Agora é possível indicar quais arquivos de instalação podem passar o atributo de pacote de instalação confiável da cadeia inteira de arquivos extraídos deles. Isso permite aumentar a estabilidade dos processos de instalação de software em um computador com o Controle de Inicialização de Aplicativos ativado, mas também expande a área para um ataque em potencial aumentando o número de inicializações de aplicativos autorizadas. Recomenda-se usar esta opção durante as implantações de software complexos, inclusive quando o computador deve ser reiniciado durante o processo de distribuição de software.
- Integração com ferramentas WMI.

  Agora, quando o aplicativo é instalado, um namespace Kaspersky Security é criado automaticamente no namespace da raiz WMI no computador local. É possível usar soluções cliente compatíveis com consultas WMI para obter dados sobre o aplicativo e os seus componentes.
- O formato para exibir informações sobre o aplicativo e os seus componentes foi expandido com o comando KAVSHELL OMSINFO: agora você pode adquirir informações sobre o status da tarefa de Controle de Inicialização de Aplicativos, bem como informações sobre atualizações críticas instaladas de módulos do aplicativo.
- Possibilidades melhoradas para gerenciar e monitorar o estado do aplicativo usando a Interface de Diagnóstico Compacta:
  - Agora é possível revisar os contadores estatísticos para componentes instalados na guia Estatísticas da Interface de Diagnóstico Compacta.
  - A senha não é necessária para acessar a Interface de Diagnóstico Compacta, mesmo se o recurso de proteção por senha estiver ativo: o aplicativo limita o acesso às informações e elementos de controle disponíveis na Interface de Diagnóstico Compacta, com base apenas nas permissões de usuário especificadas para o gerenciamento de aplicativo.
- A partir da versão 2.2, o aplicativo implementa a capacidade de fornecer proteção básica do computador durante a inicialização de sistema operacional no modo seguro.

Por padrão, o aplicativo não funciona em um computador em modo seguro. Para inicializar o aplicativo quando o sistema operacional for iniciado no modo seguro, configure o parâmetro LoadInSafeMode como 1 na seguinte chave do registro do Windows:

`HKLM\SYSTEM\CurrentControlSet\services\klam\Parameters`

> Ao ser executado em um computador iniciado no modo seguro, a funcionalidade do aplicativo será limitada.

- Relatórios do Kaspersky Security Center compatíveis: você agora pode revisar relatórios do status de componentes do aplicativo e dois tipos de relatórios sobre aplicativos proibidos.

  Esta funcionalidade é compatível apenas quando estiver usando Kaspersky Security Center 11.
- As permissões de acesso de usuário para alterar a pasta Instalação e modificar bifurcações de registro críticas dos componentes do aplicativo agora são limitadas.

Kit de distribuição

O kit de distribuição inclui o aplicativo de boas-vindas que permite executar as seguintes ações:

- Iniciar o Assistente de instalação do Kaspersky Embedded Systems Security 2.2.
- Iniciar o Assistente de instalação do Console do Kaspersky Embedded Systems Security 2.2.
- Iniciar o Assistente de instalação que instalará o Plug-in de Administração do Kaspersky Embedded Systems Security 2.2 para gerenciar o aplicativo por meio do Kaspersky Security Center.
- Ler o Manual do Administrador.
- Ler o Manual do Usuário.
- Acessar a página do Kaspersky Embedded Systems Security 2.2 no site da Kaspersky Lab.
- Visitar o site do Suporte Técnico (https://support.kaspersky.com.br/).
- Ler as informações sobre a versão atual do Kaspersky Embedded Systems Security 2.2.

A pasta \console contêm arquivos para instalação do Console do Aplicativo (conjunto de componentes “Ferramentas de Administração do Kaspersky Embedded Systems Security 2.2”).

A pasta \product contém:

- Arquivos para a instalação dos componentes do Kaspersky Embedded Systems Security 2.2 em um computador que executa o sistema operacional Microsoft Windows de 32 bits ou de 64 bits.
- Arquivo para a instalação do Plug-in de Administração para gerenciar o Kaspersky Embedded Systems Security 2.2 por meio do Kaspersky Security Center.
- Arquivo compactado de bancos de dados de antivírus atuais no momento do lançamento do aplicativo.
- Arquivo com o texto do Contrato de Licença do Usuário Final e Política de Privacidade.

A pasta \product_no_avbases contém arquivos de instalação de componentes e plug-ins do Kaspersky Embedded Systems Security 2.2 sem os bancos de dados de antivírus.

A pasta \setup contém os arquivos de inicialização do programa de boas-vindas.

Os arquivos do kit de distribuição são armazenados em pastas diferentes, dependendo do uso pretendido (consulte a tabela abaixo).

Tabela 2. Arquivos do kit de distribuição do Kaspersky Embedded Systems Security 2.2

Arquivo	Finalidade
autorun.inf	Arquivo de execução automática para o Assistente de instalação do Kaspersky Embedded Systems Security 2.2 ao instalar o aplicativo a partir de mídias removíveis.
ess_admin_guide_pt.pdf	Manual do Administrador.
ess_user_guide_pt.pdf	Manual do Usuário.
release_notes.txt	O arquivo contém informações da versão.
setup.exe	Arquivo de inicialização do programa de boas-vindas (inicia setup.hta).
\console\esstools_x86(x64).msi	Pacote de instalação de Instalador do Windows; instala o Console do Aplicativo no computador protegido.
\console\setup.exe	O arquivo que inicia o assistente de configuração para o conjunto de componentes "Ferramentas de administração" (incluindo o Console do Aplicativo); inicia o arquivo do pacote de instalação esstools.msi usando as configurações especificadas no assistente de configuração.
\product\bases.cab	Arquivo comprimido dos bancos de dados de antivírus atuais do antivírus no momento da liberação do aplicativo.
\product\setup.exe	O arquivo que inicia o assistente para instalar o Kaspersky Embedded Systems Security 2.2 no computador protegido; inicia o arquivo do pacote de instalação ess.msi com as configurações de instalação especificadas no assistente.
\product\ess_x86(x64).msi	Pacote de instalação do Windows Installer; instala o Kaspersky Embedded Systems Security 2.2 no computador protegido.
\product\ess.kud	Arquivo no formato Kaspersky Unicode Definition com uma descrição do pacote de instalação para a instalação remota do Kaspersky Embedded Systems Security 2.2 por meio do Kaspersky Security Center.
\product\klcfginst.exe	Instalador do Plug-in de Administração para gerenciar o Kaspersky Embedded Systems Security 2.2 por meio do Kaspersky Security Center. Instale o Plug-in de Administração em cada computador em que o Console de Administração do Kaspersky Security Center está instalado se planejar usá-lo para gerenciar o Kaspersky Embedded Systems Security 2.2.
\product\license.txt	Texto do Contrato de Licença do Usuário Final e da Política de Privacidade.
\product\migration.txt	O arquivo descreve a migração de versões anteriores do aplicativo.
\setup\setup.hta	Arquivo de inicialização do programa de boas-vindas.

Os arquivos do kit de distribuição podem ser executados a partir do CD de instalação. Caso você tenha copiado os arquivos do pacote de distribuição para a unidade local antes, certifique-se de que a estrutura dos arquivos do kit de distribuição foi mantida.

Requisitos de hardware e software

Antes de instalar o Kaspersky Embedded Systems Security 2.2, você deve desinstalar outros aplicativos antivírus do computador.

Requisitos de hardware para o computador protegido

Requisitos gerais:

- sistemas compatíveis com x86 em configurações com um ou vários processadores.
- sistemas compatíveis com x64 em configurações com um ou vários processadores.

Volume do disco:

- para instalar o componente de Controle de Inicialização de Aplicativos – 50 MB
- para instalar todos os componentes do Kaspersky Embedded Systems Security 2.2 – 500 MB

RAM:

- 256 MB para instalar o componente do Controle de Inicialização de Aplicativos apenas no computador com sistema operacional Microsoft® Windows;
- 512 MB para realizar a instalação completa de todos os componentes no computador com sistema operacional Microsoft Windows.

Exigências mínimas de processador:

- para sistemas operacionais Microsoft Windows de 32 bits: Intel® Pentium® III.
- para sistemas operacionais Microsoft Windows de 64 bits: Intel Pentium IV.

Requisitos de software para o computador protegido

Você pode instalar o Kaspersky Embedded Systems Security 2.2 em um dispositivo com sistema operacional Microsoft Windows de 32 ou 64 bits.

O Windows Installer 3.1 é necessário para uma instalação e funcionamento adequados do aplicativo em um computador com sistema operacional Microsoft Windows XP.

Para instalar e usar o Kaspersky Embedded Systems Security 2.2 nos dispositivos com sistemas operacionais incorporados, são necessários os componentes das Ferramentas de Suporte à Administração e Gerenciador de Filtro.

Você pode instalar o Kaspersky Embedded Systems Security 2.2 em um computador com um dos seguintes sistemas operacionais Microsoft Windows de 32 ou 64 bits:

- Windows XP Embedded SP3
- Windows XP Pro SP2/SP3
- Windows Embedded POSReady 2009
- Windows Embedded Standard 7 SP1
- Windows Embedded Enterprise 7 SP1

- Windows Embedded POSReady 7
- Windows 7 Professional / Enterprise SP1
- Windows Embedded 8.1 Industry Professional / Enterprise
- Windows Embedded 8.1 Professional
- Windows Embedded 8.0 Standard
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise
- Windows 10 IoT Enterprise
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise

Instalação e remoção do aplicativo

Esta seção fornece instruções passo a passo para instalar e remover o Kaspersky Embedded Systems Security 2.2.

Neste capítulo

Componentes de software do Kaspersky Embedded Systems Security 2.2 e seus códigos para o serviço do Windows Installer

Por padrão, os arquivos \server\ess_x86(x64).msi destinam-se a instalar todos os componentes do Kaspersky Embedded Systems Security 2.2. Você pode instalar este componente incluindo-o em uma instalação personalizada.

Os arquivos \client\esstools_x86(x64).msi instalam todos os componentes de software a partir do conjunto de "Ferramentas Administrativas".

As seções a seguir enumeram os códigos dos componentes do Kaspersky Embedded Systems Security 2.2 para o serviço do Windows Installer. Estes códigos podem ser usados para definir uma lista de componentes a serem instalados ao instalar o Kaspersky Embedded Systems Security 2.2 a partir da linha de comando.

Nesta seção

Componentes de software do Kaspersky Embedded Systems Security 2.2

A tabela a seguir contém os códigos e uma descrição dos componentes de software do Kaspersky Embedded Systems Security 2.2.

Tabela 3. Descrição dos componentes de software do Kaspersky Embedded Systems Security 2.2

Componente	Código	Funções realizadas
Funcionalidade básica	Core	Este componente contém o conjunto de funções básicas do aplicativo e assegura a sua operação.
Controle de Inicialização de Aplicativos	AppCtrl	Este componente monitora tentativas de usuário de executar aplicativos e permite ou nega a inicialização deles conforme as regras de Controle de Inicialização de Aplicativos definidas. É implementado na tarefa de Controle de Inicialização de Aplicativos.
Controle de Dispositivos	DevCtrl	Este componente rastreia tentativas de conexão de dispositivos de armazenamento em massa via USB a um computador protegido e permite ou proíbe o uso desses dispositivos de acordo com as regras de controle de dispositivos especificadas. O componente é implementado na tarefa de Controle de Dispositivos.
Proteção antivírus	AVProtection	Este componente assegura a proteção de antivírus e contém os componentes a seguir: • Verificação por Demanda • Proteção de Arquivos em Tempo Real
Verificação por Demanda	Ods	Este componente instala arquivos de sistema do Kaspersky Embedded Systems Security 2.2 e tarefas de Verificação por Demanda (verificação de objetos no computador protegido mediante solicitação). Se outros componentes do Kaspersky Embedded Systems Security 2.2 forem especificados durante a instalação do Kaspersky Embedded Systems Security 2.2 a partir da linha de comando, mas o componente Core não for especificado, o componente Core será instalado automaticamente.
Proteção de Arquivos em Tempo Real	Oas	Este componente executa verificações de antivírus de arquivos no computador protegido quando estes arquivos são acessados. Ele implementa a tarefa de Proteção de Arquivos em Tempo Real.

Componente	Código	Funções realizadas
Uso da Kaspersky Security Network	KSN	Este componente fornece a proteção com base em tecnologias na nuvem da Kaspersky Lab. Ele implementa a tarefa de Uso da KSN (enviando solicitações para e recebendo conclusões do serviço Kaspersky Security Network).
Monitor de Integridade de Arquivos	Fim	Este componente registra as operações executadas em arquivos no escopo do monitoramento especificado. O componente implementa a tarefa do Monitor de Integridade de Arquivos.
Prevenção de Exploits	AntiExploit	Este componente possibilita gerenciar as configurações para proteger a memória utilizada pelos processos na memória de um computador protegido.
Gerenciamento de Firewall	Firewall	Este componente possibilita gerenciar o Firewall do Windows por meio da interface gráfica do usuário do Kaspersky Embedded Systems Security 2.2. O componente implementa a tarefa de Gerenciamento de Firewall.
Módulo para integração com o Agente de Rede do Kaspersky Security Center	AKIntegration	Fornece uma conexão entre o Kaspersky Embedded Systems Security 2.2 e o Agente de Rede do Kaspersky Security Center. Você pode instalar este componente no computador protegido caso pretenda gerenciar o aplicativo através do Kaspersky Security Center.
Inspeção do Log	LogInspector	Este componente monitora a integridade do ambiente protegido com base nos resultados de uma inspeção dos logs de evento do Windows.
Conjunto de contadores de desempenho do "Monitor do Sistema"	PerfMonCounters	Este componente instala um conjunto de contadores de desempenho do Monitor do Sistema. Os contadores de desempenho ativam o desempenho do Kaspersky Embedded Systems Security 2.2 a ser medido e gargalos potenciais a ser localizados no computador quando o Kaspersky Embedded Systems Security 2.2 for usado com outros programas.
Contadores e interceptações SNMP	SnmpSupport	Este componente publica contadores e interceptações do Kaspersky Embedded Systems Security 2.2 por meio do Simple Network Management Protocol (SNMP) no Microsoft Windows. Este componente pode ser instalado no computador protegido somente se o Microsoft SNMP for instalado no mesmo computador.

Componente	Código	Funções realizadas
Ícone do Kaspersky Embedded Systems Security 2.2 na área de notificação	TrayApp	Este componente exibe o ícone do Kaspersky Embedded Systems Security 2.2 na área de notificação da bandeja de tarefas do computador protegido. O ícone do Kaspersky Embedded Systems Security 2.2 exibe o status da proteção do computador e pode ser usado para abrir o Console do Kaspersky Embedded Systems Security 2.2 no Console de Gerenciamento Microsoft (se instalado) e na janela **Sobre o aplicativo**.
Utilitário de linha de comando	Shell	Permite controlar o Kaspersky Embedded Systems Security 2.2 a partir da linha de comando de um computador protegido.

Conjunto de “Ferramentas de administração” de componentes de software

A tabela a seguir contém códigos para o conjunto de “Ferramentas de administração” e uma descrição dos seus componentes de software.

Tabela 4. Descrição dos componentes de software das "Ferramentas de administração"

Componente	Código	Funções do componente
Snap-ins do Kaspersky Embedded Systems Security 2.2	MmcSnapin	Este componente instala o snap-in do Console de Gerenciamento da Microsoft por meio do Console do Kaspersky Embedded Systems Security 2.2. Se outros componentes forem especificados durante a instalação das “Ferramentas de administração” a partir da linha de comando e o componente MmcSnapin não for especificado, o componente será instalado automaticamente.
Ajuda	Help	Arquivo de ajuda .chm, salvo na pasta com os arquivos das Ferramentas de administração do Kaspersky Embedded Systems Security 2.2. Você pode abrir o arquivo de Ajuda usando o menu **Iniciar** ou clicando na tecla **F1** com a janela do Console do Aplicativo aberta.
Documentação	Help	O Kaspersky Embedded Systems Security 2.2 adiciona um atalho ao recurso da web da Kaspersky Lab onde o Manual do Administrador e o Manual do Usuário estão disponíveis em formato PDF. O atalho está disponível no menu Iniciar.

Modificações de sistema após a instalação do Kaspersky Embedded Systems Security 2.2

Quando o Kaspersky Embedded Systems Security 2.2 e o Console do Aplicativo (conjunto de "Ferramentas de administração") são instalados juntos, o serviço do Windows Installer fará as seguintes modificações no computador protegido:

- Cria as pastas do Kaspersky Embedded Systems Security 2.2 no computador protegido e no computador em que o Console do Aplicativo for instalado.
- Registra os serviços do Kaspersky Embedded Systems Security 2.2.
- Cria um grupo de usuários do Kaspersky Embedded Systems Security 2.2.
- Registra chaves do Kaspersky Embedded Systems Security 2.2 no registro do sistema.

Essas alterações estão descritas na tabela abaixo.

Pastas do Kaspersky Embedded Systems Security 2.2

Tabela 5. Pastas do Kaspersky Embedded Systems Security 2.2 em um computador protegido

Pasta	Arquivos do Kaspersky Embedded Systems Security 2.2
Pasta de instalação padrão do Kaspersky Embedded Systems Security 2.2: Na versão de 32 bits do Microsoft Windows – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\ Na versão de 64 bits do Microsoft Windows – %ProgramFiles(x86)%\Kaspersky Embedded Systems Security\	Arquivos executáveis do Kaspersky Embedded Systems Security 2.2 (pasta de destino especificada durante a instalação).
Pasta %Kaspersky Embedded Systems Security%\mibs	Arquivos de Management Information Base (MIB); estes arquivos contêm uma descrição dos contadores e hooks publicados pelo Kaspersky Embedded Systems Security 2.2 por meio do protocolo SNMP.
Pasta %Kaspersky Embedded Systems Security%\x64	As versões de 64 bits dos arquivos executáveis do Kaspersky Embedded Systems Security 2.2 (a pasta será criada apenas durante a instalação do Kaspersky Embedded Systems Security 2.2 na versão de 64 bits do Microsoft Windows).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Embedded Systems Security\2.2\Dskm\	Arquivos de serviço do Kaspersky Embedded Systems Security 2.2.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\	Arquivos com configurações das fontes de atualização.

Pasta	Arquivos do Kaspersky Embedded Systems Security 2.2
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\Distribution\	Atualizações de bancos de dados e módulos de software baixados usando a tarefa Copiar atualizações (a pasta será criada na primeira vez que as atualizações forem baixadas usando a tarefa Copiar atualizações).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Reports\	Logs de tarefas e log de auditoria do sistema.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Current\	Conjunto de bancos de dados usados na hora atual.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Backup\	Cópia de backup dos bancos de dados; serão sobrescritas sempre que os bancos de dados forem atualizados.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Temp\	Arquivos temporários criados durante a execução das tarefas de atualização.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Quarantine\	Objetos na Quarentena (pasta padrão).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Backup\	Objetos no backup (pasta padrão).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored\	Objetos restaurados do backup e da quarentena (pasta padrão para objetos restaurados).

Tabela 6. Pastas criadas durante a instalação do Console do Aplicativo

Pasta	Arquivos do Console do Kaspersky Embedded Systems Security 2.2
Pasta de instalação padrão do Console do Aplicativo: • Na versão do Microsoft Windows de 32 bits – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\ • Na versão do Microsoft Windows de 64 bits – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\	Arquivos das "Ferramentas de administração" (pasta de destino especificada durante a instalação do Console do Kaspersky Embedded Systems Security 2.2).

Serviços do Kaspersky Embedded Systems Security 2.2

Os serviços do Kaspersky Embedded Systems Security 2.2 começam utilizando a conta do Sistema local (SISTEMA).

Tabela 7. Serviços do Kaspersky Embedded Systems Security 2.2

Serviço	Finalidade
Kaspersky Security Service (KAVFS)	Serviço essencial do Kaspersky Embedded Systems Security 2.2 que gerencia tarefas e fluxos de trabalho do Kaspersky Embedded Systems Security 2.2.
Kaspersky Security Management Service (KAVFSGT)	O serviço é destinado ao gerenciamento de aplicativos do Kaspersky Embedded Systems Security 2.2 por meio do Console do Aplicativo.

Grupos do Kaspersky Embedded Systems Security 2.2

Tabela 8. Grupos do Kaspersky Embedded Systems Security 2.2

Grupo	Finalidade
Administradores de ESS	Um grupo no computador protegido cujos usuários têm acesso total ao Kaspersky Security Management Service e a todas as funções do Kaspersky Embedded Systems Security 2.2.

Chaves do registro do sistema

Tabela 9. Chaves do registro do sistema

Chave	Finalidade
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Propriedades do serviço do Kaspersky Embedded Systems Security 2.2.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Configurações do log de eventos do Kaspersky Embedded Systems Security 2.2 (Log de Eventos Kaspersky).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Propriedades do serviço de gerenciamento do Kaspersky Embedded Systems Security 2.2.
Na versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance] Na versão de 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance].	Configurações dos contadores de desempenho.
Na versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\SnmpAgent] Na versão de 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\SnmpAgent]	Configurações do componente de Suporte do Protocolo SNMP.

Chave	Finalidade
Na versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\CrashDump] Na versão de 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\CrashDump]	Configurações de gravação de arquivo de despejo.
Na versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\Trace] Na versão de 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Trace]	Configurações do arquivo de rastreamento.
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Environment]	Configuração das tarefas e funções do aplicativo.

Processos do Kaspersky Embedded Systems Security 2.2

O Kaspersky Embedded Systems Security 2.2 inicia os processos descritos na tabela abaixo.

Tabela 10. Processos do Kaspersky Embedded Systems Security 2.2

Nome do arquivo	Finalidade
kavfswp.exe	Fluxo de trabalho do Kaspersky Embedded Systems Security 2.2
kavtray.exe	Processo para ícone de bandeja do sistema
kavshell.exe	Processo do utilitário de linha de comando
kavfsrcn.exe	Processo de gerenciamento remoto do Kaspersky Embedded Systems Security 2.2
kavfs.exe	Processo do Kaspersky Security Service
kavfsgt.exe	Processos do Kaspersky Security Management Service
kavfswh.exe	Processo do Serviço de Prevenção de Exploits do Kaspersky Security

Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer

As tabelas apresentadas abaixo contêm descrições das configurações para a instalação e desinstalação do Kaspersky Embedded Systems Security 2.2, seus valores padrão, chaves para alterar os valores das configurações de instalação e seus valores possíveis. Essas chaves podem ser usadas em conjunto com as chaves padrão para o comando msiexec do serviço do Windows Installer ao instalar o Kaspersky Embedded Systems Security 2.2 a partir da linha de comando.

Tabela 11. Parâmetros de instalação e opções da linha de comando no Windows Installer

Configuração	Opções da linha de comando do Windows Installer e seus valores possíveis	Valor padrão	Descrição
Aceitação dos termos do Contrato de Licença do Usuário Final	EULA=<value> 0 – você não aceita os termos do Contrato de Licença do Usuário Final. 1 – você aceita os termos do Contrato de Licença do Usuário Final.	0	Você deve aceitar os termos do Contrato de Licença do Usuário Final para instalar o Kaspersky Embedded Systems Security 2.2.
Aceitação dos termos de Política de Privacidade	PRIVACYPOLICY=<value> 0 – você não aceita os termos da Política de Privacidade. 1 – você aceita os termos da Política de Privacidade.	0	Você deve aceitar que os termos da Política de Privacidade para instalar o Kaspersky Embedded Systems Security 2.2.
Pasta de destino	INSTALLDIR=<caminho completo para a pasta>	Kaspersky Embedded Systems Security 2.2: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Ferramentas de administração: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools Na versão de x64 bits do Microsoft Windows: %ProgramFiles(x86)%.	Pasta em que os arquivos do Kaspersky Embedded Systems Security 2.2 serão salvos durante a instalação. Uma pasta diferente pode ser especificada.

Configuração	Opções da linha de comando do Windows Installer e seus valores possíveis	Valor padrão	Descrição
Inicialização da tarefa de Proteção de Arquivos em Tempo Real quando o Kaspersky Embedded Systems Security 2.2 é iniciado (**Ativar a proteção em tempo real após a instalação do aplicativo**)	RUNRTP=<valor> 1 – iniciar; 0 – não iniciar.	1	Ative esta configuração para iniciar a Proteção de Arquivos em Tempo Real na inicialização do Kaspersky Embedded Systems Security 2.2 (recomendado).
Exclusões da verificação conforme recomendado pela Microsoft Corporation (**Adicionar arquivos recomendados pela Microsoft à lista de exclusões**)	ADDMSEXCLUSION=<valor> 1 – excluir; 0 – não excluir.	1	Na tarefa Proteção de Arquivos em Tempo Real, exclua do escopo da proteção objetos no computador que são recomendados pela Microsoft Corporation para exclusão. Alguns aplicativos no computador podem ficar instáveis quando o aplicativo de antivírus interceptar ou modificar arquivos usados por esses aplicativos. Por exemplo, a Microsoft Corporation inclui alguns aplicativos de controladores de domínio na lista de tais objetos.
Objetos excluídos do escopo da verificação segundo as recomendações da Kaspersky Lab (**Adicionar arquivos recomendados pela Kaspersky à lista de exclusões**)	ADDKLEXCLUSION=<valor> 1 – excluir; 0 – não excluir.	1	Na tarefa Proteção de Arquivos em Tempo Real, exclua do escopo da proteção objetos no computador que são recomendados pela Kaspersky Lab para exclusão.

Configuração	Opções da linha de comando do Windows Installer e seus valores possíveis	Valor padrão	Descrição
Permitir a conexão remota ao Console do Aplicativo.	ALLOWREMOTECON=<valor> 1 – permitir; 0 – negar.	0	Por padrão, a conexão remota ao Console do Aplicativo instalado no computador protegido não é permitida. Durante a instalação, você pode permitir a conexão. O Kaspersky Embedded Systems Security 2.2 cria regras de permissão para o processo kavfsgt.exe usando o protocolo TCP para todas as portas.
Caminho do arquivo de chave (**Chave**)	LICENSEKEYPATH=<nome do arquivo da chave>	Diretório \product no kit de distribuição	Por padrão, o instalador tenta encontrar o arquivo com a extensão .key na pasta \product do kit de distribuição. Se a pasta \product contiver vários arquivos de chave, o instalador irá selecionar o arquivo de chave que terá a data de expiração mais longa. Um arquivo de chave pode ser salvo antecipadamente na pasta \product ou especificando outro caminho para o arquivo de chave usando a configuração **Adicionar chave**.
			É possível adicionar uma chave depois que o Kaspersky Embedded Systems Security 2.2 for instalado usando uma ferramenta de administração de sua escolha: por exemplo, o Console do Aplicativo. Se você não adicionar uma chave durante a instalação do aplicativo, o Kaspersky Embedded Systems Security 2.2 não funcionará.

Configuração	Opções da linha de comando do Windows Installer e seus valores possíveis	Valor padrão	Descrição
Caminho do arquivo de configuração	CONFIGPATH=<nome do arquivo de configuração>	Não especificado	O Kaspersky Embedded Systems Security 2.2 importa configurações do arquivo de configuração especificado criado no aplicativo. O Kaspersky Embedded Systems Security 2.2 não importa senhas do arquivo de configuração, por exemplo, senhas de contas para tarefas de inicialização ou senhas para conexão com um servidor proxy. Com configurações importadas, você terá que inserir todas as senhas manualmente. Se o arquivo de configuração não for especificado, o aplicativo começará a trabalhar com as configurações padrão após a configuração.

Configuração	Opções da linha de comando do Windows Installer e seus valores possíveis	Valor padrão	Descrição
Ativando conexões de rede para o Console	ADDWFEXCLUSION=<valor> **1** – permitir; **0** – negar.	0	Use esta opção para instalar o Kaspersky Embedded Systems Security 2.2 em outro computador. É possível gerenciar remotamente uma proteção de computador a partir de outro dispositivo com o Console do Kaspersky Embedded Systems Security 2.2 instalado. A porta 135 (TCP) é aberta no Firewall do Microsoft Windows, são permitidas as conexões de rede para o arquivo executável kavfsrcn.exe para o gerenciamento remoto do Kaspersky Embedded Systems Security 2.2 e o acesso é concedido aos aplicativos DCOM. Após a conclusão da instalação, adicione usuários ao grupo Administradores de ESS para permitir o gerenciamento remoto de aplicativos e conexões de rede ao Kaspersky Security Management Service (arquivo kavfsgt.exe) no computador. Você pode ler mais sobre a configuração adicional quando o Console do Kaspersky Embedded Systems Security 2.2 for instalado em outro computador (consulte a Seção "Configurações avançadas após a instalação do Console do Aplicativo em outro computador" na página 44).

Configuração	Opções da linha de comando do Windows Installer e seus valores possíveis	Valor padrão	Descrição
Desativação da verificação de software incompatível	SKIPINCOMPATIBLESW = <valor> 0 - A verificação de software incompatível é realizada 1 - A verificação de software incompatível não é realizada	0	Use esta configuração para ativar ou desativar a verificação de software incompatível durante a instalação em segundo plano do aplicativo no dispositivo. Independentemente do valor dessa configuração, durante a instalação do Kaspersky Embedded Systems Security 2.2, o aplicativo sempre alerta sobre outras versões do aplicativo instalado no dispositivo.

Tabela 12. Configurações de desinstalação e opções da linha de comando no Windows Installer

Configuração	Opções da linha de comando do Windows Installer e seus valores possíveis	Valor padrão
Restaurando objetos da Quarentena	RESTOREQTN =<valor> **0** – excluir o conteúdo em Quarentena; **1** – restaurar o conteúdo em Quarentena à pasta especificada pelo parâmetro RESTOREPATH na subpasta \Quarantine.	0 – Remover
Restaurando o conteúdo do backup	RESTOREBCK =<valor> **0** – excluir o conteúdo do backup; **1** – restaurar o conteúdo do backup à pasta especificada pelo parâmetro RESTOREPATH na subpasta \Backup.	0 – Remover
Insira a senha atual para confirmar a exclusão (se a proteção de senha estiver ativa)	UNLOCK_PASSWORD=<senha especificada>	Não especificado
Pasta para a objetos restaurados	RESTOREPATH=<caminho completo para a pasta> Objetos restaurados serão salvos na pasta especificada:	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored

Log de instalação e desinstalação do Kaspersky Embedded Systems Security 2.2

Se o Kaspersky Embedded Systems Security 2.2 for instalado ou desinstalado usando o Assistente de instalação (Desinstalação), o serviço do Windows Installer cria um log de instalação (desinstalação). O arquivo de log ess_install_<uid>.log (onde <uid> – identificador de log único de 8 caracteres) será salvo em uma pasta %temp% do usuário de cuja conta o arquivo setup.exe foi iniciado.

Se você executar a opção **Modificar ou Remover** para o Console do Aplicativo ou o Kaspersky Embedded Systems Security 2.2 a partir do menu **Iniciar**, ess_2.2_maintenance.log é criado automaticamente na pasta %temp%.

Se o Kaspersky Embedded Systems Security 2.2 for instalado ou desinstalado a partir da linha de comando, o log do arquivo de instalação não será criado por padrão.

► *Para instalar o Kaspersky Embedded Systems Security 2.2 com o arquivo de log criado no disco C:\:*

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

Planejamento da instalação

Esta seção contém a descrição do conjunto de Ferramentas de administração do Kaspersky Embedded Systems Security 2.2 e de aspectos especiais de instalação e desinstalação do Kaspersky Embedded Systems Security 2.2 usando um assistente (consulte a seção "Instalação e desinstalação do aplicativo usando um assistente" na página 40), a linha de comando (consulte a seção "Instalação e desinstalação do aplicativo a partir da linha de comando" na página 52), por meio do Kaspersky Security Center (consulte a seção "Instalação e desinstalação do aplicativo usando o Kaspersky Security Center" na página 57) e por meio da política de grupo do Active Directory® (consulte a seção "Instalação e desinstalação via políticas de grupo do Active Directory" na página 61).

Antes de iniciar a instalação do Kaspersky Embedded Systems Security 2.2, planeje suas etapas principais.

1. Determine que ferramentas de administração serão usadas para gerenciar e configurar o Kaspersky Embedded Systems Security 2.2.
2. Selecione os componentes necessários do aplicativo para instalação (consulte a seção "Componentes de software do Kaspersky Embedded Systems Security 2.2 e seus códigos para o serviço do Windows Installer" na página 23).
3. Selecione o método de instalação.

Nesta seção

Seleção das ferramentas de administração

Determine as ferramentas de administração que serão usadas para configurar o Kaspersky Embedded Systems Security 2.2 e gerenciá-lo. O Kaspersky Embedded Systems Security 2.2 pode ser gerenciado usando o Console do Aplicativo, o utilitário de linha de comando e o Console de Administração do Kaspersky Security Center.

Console do Kaspersky Embedded Systems Security 2.2

O Console do Kaspersky Embedded Systems Security 2.2 é um snap-in isolado adicionado ao Console de Gerenciamento da Microsoft. O Kaspersky Embedded Systems Security 2.2 pode ser gerenciado por meio do Console do Aplicativo instalado no computador protegido ou em outro computador da rede corporativa.

Vários snap-ins do Kaspersky Embedded Systems Security 2.2 podem ser adicionados a um Console de Gerenciamento da Microsoft aberto no modo de autor para utilizá-lo para gerenciar a proteção de vários computadores nos quais o Kaspersky Embedded Systems Security 2.2 está instalado.

O Console do Aplicativo está incluído no conjunto de componentes "Ferramentas de administração" do aplicativo.

Utilitário de linha de comando

Você pode gerenciar o Kaspersky Embedded Systems Security 2.2 a partir da linha de comando de um computador protegido.

O utilitário de linha de comando está incluído no grupo dos componentes do software Kaspersky Embedded Systems Security 2.2.

Kaspersky Security Center

Se o aplicativo Kaspersky Security Center for usado para o gerenciamento centralizado da proteção antivírus de computadores na sua empresa, você poderá gerenciar o Kaspersky Embedded Systems Security 2.2 por meio do Console de Administração do Kaspersky Security Center.

Os componentes a seguir devem ser instalados:

- **Módulo para a integração com o Agente de Rede do Kaspersky Security Center**. Este componente está incluído no grupo dos componentes do software do Kaspersky Embedded Systems Security 2.2. Ele garante a comunicação do Kaspersky Embedded Systems Security 2.2 com o Agente de Rede. Instale o módulo para a integração com o Agente de Rede do Kaspersky Security Center no computador protegido.
- **Agente de Rede do Kaspersky Security Center**. Instale este componente em cada computador protegido. Este componente é compatível com a interação entre o Kaspersky Embedded Systems Security 2.2 instalado no computador e o Console de Administração do Kaspersky Security Center. O arquivo de instalação do Agente de Rede está incluído na pasta do kit de distribuição do Kaspersky Security Center.
- **Plug-in de Administração do Kaspersky Embedded Systems Security 2.2**. Adicionalmente, instale o Plug-in de Administração do Kaspersky Embedded Systems Security 2.2 por meio do Console de Administração no computador em que o Servidor de Administração do Kaspersky Security Center estiver instalado. Isso garante a interface de gerenciamento de aplicativos através do Kaspersky Security Center. O arquivo de instalação do Plug-in de Administração, \product\klcfginst.exe, está incluído no kit de distribuição do Kaspersky Embedded Systems Security 2.2.

Seleção do tipo de instalação

Depois de especificar os componentes de software para a instalação do Kaspersky Embedded Systems Security 2.2 (consulte a seção "Componentes de software do Kaspersky Embedded Systems Security 2.2 e seus códigos para o serviço do Windows Installer" na página 23), será necessário selecionar o método de instalação do aplicativo.

Selecione o método de instalação dependendo da arquitetura de rede e das seguintes condições:

- Se configurações especiais de instalação precisarem ser definidas para o Kaspersky Embedded Systems Security 2.2 ou se as configurações de instalação recomendadas (consulte a seção "Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer" na página 30) serão usadas.
- As configurações de instalação serão as mesmas para todos os computadores ou específicas para cada um deles.

O Kaspersky Embedded Systems Security 2.2 pode ser instalado interativamente usando o Assistente de instalação ou em modo silencioso sem a participação do usuário e chamado executando o arquivo do pacote de instalação com as configurações de instalação na linha de comando. Uma instalação remota centralizada do Kaspersky Embedded Systems Security 2.2 pode ser executada usando políticas de grupo do Active Directory ou usando a tarefa de instalação remota do Kaspersky Security Center.

O Kaspersky Embedded Systems Security 2.2 pode ser instalado em um computador único, configurado para operação e suas configurações salvas em um arquivo de configuração; o arquivo criado pode então ser usado para instalar o Kaspersky Embedded Systems Security 2.2 em outro computador (essa possibilidade não se aplica quando o aplicativo é instalado usando as políticas de grupo do Active Directory).

Inicialização do assistente de instalação

O assistente de instalação pode instalar o seguinte:

- Os componentes do Kaspersky Embedded Systems Security 2.2 (consulte a Seção "Componentes de software do Kaspersky Embedded Systems Security 2.2" na página 24) em um computador protegido a partir do arquivo \product\setup.exe incluído no kit de distribuição.
- O Console do Kaspersky Embedded Systems Security 2.2 (consulte a seção "Instalação do Console do Kaspersky Embedded Systems Security 2.2" na página 43) a partir do arquivo \client\setup.exe do kit de distribuição no computador protegido ou outro host de LAN.

Executando o arquivo do pacote de instalação a partir da linha de comando com as configurações de instalação necessárias

Se o arquivo do pacote de instalação for iniciado sem opções de linha de comando, o Kaspersky Embedded Systems Security 2.2 será instalado com as configurações padrão. As opções do Kaspersky Embedded Systems Security 2.2 podem ser usadas para modificar as configurações de instalação.

O Console do Aplicativo pode ser instalado no computador protegido e / ou na estação de trabalho do administrador.

Você também pode usar comandos de amostra para a instalação do Kaspersky Embedded Systems Security 2.2 e do Console do Aplicativo (consulte a seção "Instalação e desinstalação do aplicativo a partir da linha de comando" na página 52).

Instalação centralizada por meio do Kaspersky Security Center

Se o Kaspersky Security Center for usado em sua rede para gerenciamento de proteção antivírus de computadores em rede, o Kaspersky Embedded Systems Security 2.2 poderá ser instalado em vários computadores usando a tarefa de instalação remota do Kaspersky Security Center.

Os computadores em que você deseja instalar o Kaspersky Embedded Systems Security 2.2 por meio do Kaspersky Security Center (consulte a seção "Instalação e desinstalação do aplicativo usando o Kaspersky Security Center" na página 57) podem estar localizados no mesmo domínio do Kaspersky Security Center, bem como em um domínio diferente, ou não pertencer a nenhum domínio.

Instalação centralizada utilizando as políticas de grupo do Active Directory

As políticas de grupo do Active Directory podem ser usadas para instalar o Kaspersky Embedded Systems Security 2.2 no computador protegido. O Console do Aplicativo pode ser instalado no computador protegido ou na estação de trabalho do administrador.

O Kaspersky Embedded Systems Security 2.2 pode ser instalado usando apenas as configurações de instalação recomendadas.

Os computadores nos quais o Kaspersky Embedded Systems Security 2.2 for instalado usando políticas de grupo do Active Directory (consulte a seção "Instalação e desinstalação via políticas de grupo do Active Directory" na página 61) devem estar localizados no mesmo domínio e na mesma unidade organizacional. A instalação é realizada na inicialização do computador, antes de fazer login no Microsoft Windows.

Instalação e desinstalação do aplicativo usando um assistente

Esta seção contém a descrição do Kaspersky Embedded Systems Security 2.2 e dos processos de instalação e desinstalação do Console do Aplicativo por meio do assistente de instalação, bem como informações adicionais sobre a configuração do Kaspersky Embedded Systems Security 2.2 e ações a serem executadas após a instalação.

Nesta seção

Instalação usando o Assistente de instalação

As seções a seguir contêm informações sobre a instalação do Kaspersky Embedded Systems Security 2.2 e do Console do Aplicativo.

► *Para instalar e prosseguir com o uso do Kaspersky Embedded Systems Security 2.2, siga os passos a seguir:*

1. Instale o Kaspersky Embedded Systems Security 2.2 em um computador protegido.
2. Instale o Console do Aplicativo nos computadores dos quais você pretende gerenciar o Kaspersky Embedded Systems Security 2.2.
3. Se o Console do Aplicativo tiver sido instalado em algum computador na rede, além do computador protegido, execute o ajuste adicional para permitir que usuários do Console do Aplicativo gerenciem o Kaspersky Embedded Systems Security 2.2 remotamente.
4. Execute ações após a instalação do Kaspersky Embedded Systems Security 2.2.

Nesta seção

Instalação do Kaspersky Embedded Systems Security 2.2

Antes de instalar o Kaspersky Embedded Systems Security 2.2, siga as etapas a seguir:

- Certifique-se de que nenhum outro programa de antivírus esteja instalado no computador.
- Certifique-se de que a conta que você está utilizando para iniciar o Assistente de instalação esteja registrada no grupo de administradores no computador protegido.

Após concluir as ações descritas acima, prossiga com o procedimento de instalação. Seguindo as instruções do Assistente de instalação, especifique as configurações para a instalação do Kaspersky Embedded Systems Security 2.2. O processo de instalação do Kaspersky Embedded Systems Security 2.2 pode ser interrompido em qualquer etapa do Assistente de instalação. Para isso, pressione o botão **Cancelar** na janela do Assistente de instalação.

Você pode ler mais sobre as configurações de instalação (desinstalação) (consulte a seção "Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer" na página 30).

► *Para instalar o Kaspersky Embedded Systems Security 2.2 usando um assistente de instalação:*

1. Inicie o arquivo de boas-vindas setup.exe no computador.
2. Na janela exibida, na seção **Instalação**, clique no link **Instalar o Kaspersky Embedded Systems Security 2.2**.
3. Na tela de boas-vindas do Assistente de configuração do Kaspersky Embedded Systems Security 2.2, clique no botão **Avançar**.

   A janela **EULA e Política de Privacidade** é aberta.
4. Revise os termos do Contrato de Licença e da Política de Privacidade.
5. Se você concordar com os termos e as condições do EULA e da Política de Privacidade, selecione as caixas **os termos e as condições deste EULA** e **Política de Privacidade descrevendo o manuseio de dados** para prosseguir com a instalação.

   Se você não aceitar o EULA e/ou a Política de Privacidade, a instalação será interrompida.
6. Clique no botão **Avançar**.

   A janela **Instalação personalizada** é exibida.
7. Selecione os componentes a serem instalados.

   Por padrão, todos os componentes do Kaspersky Embedded Systems Security 2.2 estão incluídos no conjunto de instalação recomendado, exceto o componente de Gerenciamento de Firewall.

   O componente do suporte de protocolo SNMP do Kaspersky Embedded Systems Security 2.2 aparecerá somente na lista de componentes sugeridos para a instalação se o serviço do Microsoft Windows SNMP estiver instalado no computador.

8. Para cancelar todas as alterações, pressione o botão **Redefinir** na janela **Instalação personalizada**. Clique no botão **Avançar**.
9. Na janela **Selecionar pasta de destino**:
   - Se necessário, especifique uma pasta para a qual os arquivos do Kaspersky Embedded Systems Security 2.2 serão copiados.
   - Se necessário, leia as informações sobre o espaço disponível nas unidades locais clicando no botão **Disco**.

   Clique no botão **Avançar**.
10. Na janela **Configurações avançadas de instalação**, defina as seguintes configurações de instalação:
    - **Ativar a proteção em tempo real após a instalação do aplicativo**.
    - **Adicionar arquivos recomendados pela Microsoft à lista de exclusões**.
    - **Adicionar arquivos recomendados da Kaspersky Lab à lista de exclusões**.

      Clique no botão **Avançar**.
11. Na janela aberta **Importar configurações do arquivo de configuração**:
    a. Especifique o arquivo de configuração do qual importar as configurações do Kaspersky Embedded Systems Security 2.2 a partir de um arquivo de configuração existente criado em qualquer versão anterior compatível do aplicativo.
    b. Pressione o botão **Avançar**.
12. Na janela **Ativação do aplicativo**, execute uma das seguintes ações:
    - Se desejar ativar o aplicativo, especifique um arquivo de chave do Kaspersky Embedded Systems Security 2.2 para a ativação do aplicativo.
    - Se quiser ativar o aplicativo mais tarde, pressione o botão **Avançar**.
    - Se um arquivo de chave tiver sido salvo anteriormente na pasta \server do kit de distribuição, o nome desse arquivo será exibido no campo **Chave**.

      > Para adicionar a chave usando o arquivo de chave armazenado em outra pasta, especifique o arquivo de chave.

      Após o arquivo de chave ser adicionado, as informações da licença serão mostradas na janela. O Kaspersky Embedded Systems Security 2.2 exibe a data calculada da expiração da licença. O termo da licença inicia no momento em que você adiciona uma chave e expira antes da data de expiração do arquivo de chave.

      Clique no botão **Avançar** para aplicar a chave no aplicativo.
13. Na janela **Pronto para instalar**, pressione o botão **Instalar**. O assistente irá iniciar a instalação dos componentes do Kaspersky Embedded Systems Security 2.2.
14. A janela **Instalação concluída** é exibida quando a instalação for concluída.
15. Marque a caixa de seleção **Exibir Notas de Versão** para visualizar informações sobre a versão depois que o Assistente de instalação estiver concluído.
16. Clique em **OK**.

A janela do Assistente de instalação é fechada. Após a conclusão da instalação, o Kaspersky Embedded Systems Security 2.2 está pronto para uso caso a chave de ativação tenha sido adicionada.

Instalação do Console do Kaspersky Embedded Systems Security 2.2

Siga as instruções do Assistente de instalação para ajustar as configurações de instalação do Console do Aplicativo. O processo de instalação pode ser interrompido em qualquer etapa do assistente. Para isso, pressione o botão **Cancelar** na janela do Assistente de instalação.

► *Para instalar o Console do Aplicativo, siga as etapas a seguir:*

1. Certifique-se de que a conta a partir da qual você está executando o Assistente de instalação esteja incluída no grupo de administradores no computador.
2. Execute o arquivo de boas-vindas, setup.exe, no computador.

   A janela de boas-vindas é exibida.
3. Clique no link **Instalar o Console do Kaspersky Embedded Systems Security 2.2**.

   A janela de boas-vindas do Assistente de instalação é aberta. Clique no botão **Avançar**.
4. Revise os termos do Contrato de Licença do Usuário Final e Política de Privacidade na janela aberta, e selecione **os termos e as condições deste EULA** e **Política de Privacidade descrevendo o manuseio de dados** para prosseguir com a instalação. Clique no botão **Avançar**.

   A janela **Configurações avançadas de instalação** é exibida.
5. Na janela **Configurações avançadas de instalação**:
   - Se você pretende usar o Console do Aplicativo para gerenciar o Kaspersky Embedded Systems Security 2.2 instalado em um computador remoto, marque a caixa de seleção **Permitir acesso remoto**.
   - Para abrir a janela **Instalação personalizada** e selecionar componentes:
     a. Clique no botão **Avançado**.

        A janela **Instalação personalizada** é exibida.

     b. Selecione os componentes do conjunto de "Ferramentas de administração" a partir da lista.

        Por padrão, todos os componentes são instalados.

     c. Clique no botão **Avançar**.

   Você pode encontrar mais informações sobre os componentes do Kaspersky Embedded Systems Security 2.2 (consulte a seção "Componentes de software do Kaspersky Embedded Systems Security 2.2 e seus códigos para o serviço do Windows Installer" na página 23).
6. Na janela **Selecionar pasta de destino**:

   a. Se for solicitado, especifique uma pasta diferente na qual os arquivos instalados devem ser salvos.

   b. Clique no botão **Avançar**.
7. Na janela **Pronto para instalar**, pressione o botão **Instalar**.

   O assistente começará a instalação dos componentes selecionados.
8. Clique em **OK**.

A janela do Assistente de instalação é fechada. O Console do Aplicativo será instalado em um computador protegido.

Se o conjunto de “Ferramentas de administração” tiver sido instalado em algum computador da rede, além do computador protegido, ajuste as configurações avançadas (consulte a seção "Configurações avançadas após a instalação do Console do Aplicativo em outro computador" na página 44).

Configurações avançadas após a instalação do Console do Aplicativo em outro computador

Se o Console do Aplicativo tiver sido instalado em algum computador na rede, além do computador protegido, execute as ações descritas abaixo para permitir que usuários gerenciem remotamente o Kaspersky Embedded Systems Security 2.2:

- Adicione usuários do Kaspersky Embedded Systems Security 2.2 ao grupo Administradores do ESS no computador protegido.
- Permita conexões da rede para o Kaspersky Security Management Service (kavfsgt.exe) (consulte a seção "Sobre permissões de acesso para o Kaspersky Security Management Service" na página 82), se o computador protegido usar o Firewall do Windows ou um Firewall de terceiros.
- Se a caixa **Permitir acesso remoto** não for selecionada durante a instalação de Console do Aplicativo em um computador com Microsoft Windows, você deve permitir manualmente conexões de rede para o Console do Aplicativo por meio do Firewall de computador.

Permitindo conexões de rede para o Console do Aplicativo

> Os nomes de configurações podem variar dependendo do sistema operacional Windows instalado.

O Console do Aplicativo no computador remoto usa o protocolo DCOM para receber informações sobre eventos do Kaspersky Embedded Systems Security 2.2 (objetos verificados, tarefas concluídas, etc.) do Kaspersky Security Management Service no computador protegido. Você deve permitir conexões de rede para o Console do Aplicativo nas configurações do Firewall do Windows para estabelecer conexões entre o Console do Aplicativo e o Kaspersky Security Management Service.

No computador remoto, onde o Console do Aplicativo estiver instalado, faça o seguinte:

- Verifique se é permitido acesso remoto anônimo a aplicativos COM (mas não a inicialização e ativação remotas de aplicativos COM).
- No Firewall do Windows, abra a porta TCP 135 e permita conexões de rede para o arquivo executável do processo de gerenciamento remoto do Kaspersky Embedded Systems Security 2.2, kavfsrcn.exe.

  O computador cliente no qual o Console do Aplicativo está instalado usa a porta TCP 135 para acessar o computador protegido e receber resposta.
- Configure a regra de saída do Firewall do Windows para permitir a conexão.

  Diferentemente dos serviços TCP/IP e UDP/IP tradiciona.is em que um protocolo único tem uma porta fixa, o DCOM atribui portas dinamicamente aos objetos COM remotos. Se um Firewall existir entre o cliente (onde o Console do Aplicativo está instalado) e o endpoint DCOM (o servidor protegido), um grande intervalo de portas deve ser aberto.

> As mesmas etapas devem ser aplicadas para configurar qualquer outro software ou Firewall de hardware.

> Se o Console do Aplicativo tiver sido aberto enquanto você estava configurando a conexão entre o computador protegido e o computador no qual o Console do Aplicativo está instalado, feche o Console do Aplicativo, aguarde até que o processo de gerenciamento remoto do Kaspersky Embedded Systems Security 2.2, kavfsrcn.exe, seja concluído e reinicie o Console do Aplicativo. As novas configurações de conexão são aplicadas.

► *Para permitir o acesso remoto anônimo a aplicativos COM, siga as etapas a seguir:*

1. No computador remoto com o Console do Kaspersky Embedded Systems Security 2.2 instalado, abra o console de Serviços do componente.
2. Selecione **Iniciar** > **Executar**.
3. Digite o comando `dcomcnfg`.
4. Clique em **OK**.
5. Expanda o nó **Computadores** no console de **Serviços do componente** em seu computador.
6. Abra o menu de contexto no nó **Meu computador**.
7. Selecione **Propriedades**.
8. Na guia **Segurança COM** da janela **Propriedades**, clique no botão **Editar limites** no grupo de configurações **Permissões de acesso**.
9. Certifique-se de que a caixa de seleção **Permitir Acesso Remoto** esteja marcada para o usuário ANONYMOUS LOGON na janela **Permitir Acesso Remoto**.
10. Clique em **OK**.

► *Para abrir a porta TCP 135 no Firewall do Windows e permitir conexões de rede para o arquivo executável do processo de gerenciamento remoto do Kaspersky Embedded Systems Security 2.2:*

1. Feche o Console do Kaspersky Embedded Systems Security 2.2 no computador remoto.
2. Execute uma das seguintes etapas:
   - No Microsoft Windows XP ou Microsoft Windows Vista®:
     a. No Microsoft Windows XP SP2 ou posterior, selecione **Iniciar** > **Firewall do Windows**.

        No Microsoft Windows Vista, selecione **Iniciar** > **Painel de Controle** > **Firewall do Windows** e na janela **Firewall do Windows**, selecione o comando **Alterar configurações**.

     b. Na janela Firewall do Windows (ou Configurações do Firewall do Windows), clique no botão **Adicionar porta** na guia **Exclusões**.
     c. No campo **Nome**, especifique o nome da porta RPC (TCP/135) ou insira outro nome, por exemplo, Kaspersky Embedded Systems Security 2.2 DCOM, e especifique o número da porta (135) no campo **Nome da porta**.
     d. Selecione o protocolo **TCP**.
     e. Clique em **OK**.
     f. Clique no botão **Adicionar** na guia **Exclusões**.
   - No Microsoft Windows 7 ou mais recente:
     a. Selecione **Iniciar** > **Painel de Controle** > **Firewall do Windows**.
     b. Na janela **Firewall do Windows**, selecione **Permitir um programa ou recurso pelo Firewall do Windows**.
     c. Na janela **Permitir que programas comuniquem através do Firewall do Windows**, clique no botão **Permitir outro programa...**.

3. Especifique o arquivo kavfsrcn.exe na janela **Adicionar Programa**. Ele está localizado na pasta especificada como pasta de destino durante a instalação do Console do Kaspersky Embedded Systems Security 2.2 usando o Console de Gerenciamento da Microsoft.
4. Clique em **OK**.
5. Clique no botão **OK** na janela **Firewall do Windows (Configurações do Firewall do Windows)**.

► *Adicionar a regra de saída do Firewall do Windows:*

1. Selecione **Iniciar** > **Painel de Controle** > **Firewall do Windows**.
2. Na janela **Firewall do Windows**, clique no link **Configurações avançadas**.

   A janela **Firewall do Windows com Segurança Avançada** é exibida.
3. Selecione o nó filho **Regras de Saída**.
4. Clique na opção **Nova Regra** no painel **Ações**.
5. Na janela **Assistente para Nova Regra de Saída** exibida, selecione a opção **Porta** e clique em **Avançar**.
6. Selecione o protocolo **TCP**.
7. No campo **Portas remotas específicas** especifique o seguinte intervalo de portas para permitir conexões de saída: 1024-65535.
8. Na janela **Ação** selecione a opção **Permitir a conexão**.
9. Salve a nova regra e feche a janela **Firewall do Windows com Segurança Avançada**.

O Firewall do Windows agora permitirá conexões de rede entre o Console do Aplicativo e Kaspersky Security Management Service.

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 2.2

O Kaspersky Embedded Systems Security 2.2 inicia as tarefas de proteção e verificação imediatamente após a instalação se o aplicativo tiver sido ativado. Se **Ativar a proteção em tempo real após a instalação do aplicativo** (opção padrão) tiver sido selecionada durante a instalação do Kaspersky Embedded Systems Security 2.2, o aplicativo verifica os objetos do sistema de arquivos do computador quando eles forem acessados. O Kaspersky Embedded Systems Security 2.2 executará a tarefa de Verificação de Áreas Críticas todas as sextas-feiras às 20h.

Recomendamos seguir as seguintes etapas após instalar o Kaspersky Embedded Systems Security 2.2:

- Inicie a tarefa Atualização do Bancos de Dados do aplicativo. Após a instalação, o Kaspersky Embedded Systems Security 2.2 verificará objetos usando o banco de dados incluído no kit de distribuição do aplicativo.

  Recomendamos atualizar os bancos de dados do Kaspersky Embedded Systems Security 2.2 imediatamente, pois eles podem estar desatualizados.

  O aplicativo então atualizará os bancos de dados a cada hora segundo a programação padrão configurada na tarefa.

- Execute uma Verificação de Áreas Críticas no computador se nenhum software antivírus com proteção de arquivos em tempo real estiver instalado no computador protegido antes de instalar o Kaspersky Embedded Systems Security 2.2.
- Configure notificações do administrador sobre eventos do Kaspersky Embedded Systems Security 2.2.

Nesta seção

Iniciando e configurando a tarefa de atualização de bancos de dados do Kaspersky Embedded Systems Security 2.2

► *Para atualizar o banco de dados do aplicativo após a instalação, faça o seguinte:*

1. Nas configurações da tarefa de Atualização do Banco de Dados, configure uma conexão com uma fonte de atualização - Kaspersky Lab HTTP ou servidores de atualização FTP.
2. Inicie a tarefa de Atualização do Banco de Dados.

► *Para configurar a conexão com os servidores de atualização da Kaspersky Lab, na tarefa de Atualização do Banco de Dados:*

1. Inicie o Console do Aplicativo de uma das seguintes maneiras:
   - Abra o Console do Aplicativo no computador protegido. Para isso, selecione **Iniciar** > **Todos os Programas** > **Kaspersky Embedded Systems Security 2.2** > **Ferramentas de Administração** > **Console do Kaspersky Embedded Systems Security 2.2**.
   - Se o Console do Aplicativo tiver sido iniciado em um computador não protegido, conecte-se ao computador protegido:
     a. Abra o menu de contexto do nó **Kaspersky Embedded Systems Security** na árvore do Console do Aplicativo.
     b. Selecione o item **Conectar a outro computador**.
     c. Na janela **Selecionar computador**, selecione **Outro computador** e, no campo de texto, indique o nome da rede do computador protegido.

   > Se a conta você usou para efetuar login no Microsoft Windows não tiver permissões de acesso para o Kaspersky Security Management Service (consulte a seção "Sobre permissões de acesso para o Kaspersky Security Management Service" na página 82), indique uma conta com as permissões necessárias.

   A janela do Console do Aplicativo é exibida.
2. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.
3. Selecionar o nó filho **Atualização do Banco de Dados**.
4. Clique no link **Propriedades** no painel de detalhes.

5. Na janela **Configurações de tarefa** exibida, abra a guia **Configurações de conexão**.
6. Faça o seguinte:
   a. Se o Web Proxy Auto-Discovery Protocol (WPAD) não estiver configurado na sua rede para detectar automaticamente configurações de servidor proxy na LAN, especifique as configurações de servidor proxy: na seção **Configurações do servidor proxy**, marque a caixa de seleção **Usar configurações especificadas de servidor proxy**, insira o endereço no campo **Endereço** e insira o número da porta do servidor proxy no campo **Porta**.
   b. Se a sua rede necessitar de autenticação ao acessar o servidor proxy, selecione o método de autenticação necessário na lista suspensa da seção **Configurações de autenticação do servidor proxy**:
      - **Usar autenticação NTLM** se o servidor proxy suportar a autenticação NTLM integrada do Microsoft Windows. O Kaspersky Embedded Systems Security 2.2 usará a conta de usuário especificada nas configurações da tarefa para acessar o servidor proxy (por padrão a tarefa é executada na conta de usuário do **Sistema local** (**SISTEMA**)).
      - **Usar autenticação NTLM com nome de usuário e senha** se o servidor proxy for compatível com a autenticação NTLM integrada do Microsoft Windows. O Kaspersky Embedded Systems Security 2.2 usará a conta especificada para acessar o servidor proxy. Insira um nome de usuário e a senha ou selecione um usuário na lista.
      - **Aplicar nome de usuário e senha** para selecionar a autenticação básica. Insira um nome de usuário e a senha ou selecione um usuário na lista.
7. Clique em **OK** na janela **Configurações de tarefa**.

As configurações para se conectar à fonte de atualização na tarefa de Atualização do banco de dados serão salvas.

► *Para executar a tarefa de Atualização do banco de dados:*

1. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.
2. No menu de contexto no nó filho **Atualização do Banco de Dados**, selecione o item **Iniciar**.

A tarefa de Atualização do banco de dados é iniciada.

Após a tarefa ter sido concluída com sucesso, você pode visualizar a data de lançamento das últimas atualizações do banco de dados instaladas no painel de detalhes do nó **Kaspersky Embedded Systems Security**.

Verificação de Áreas Críticas

Após ter atualizado os bancos de dados do Kaspersky Embedded Systems Security 2.2, verifique o computador para a presença de malware usando a tarefa de Verificação de Áreas Críticas.

► *Para executar uma tarefa de Verificação de Áreas Críticas, siga as etapas a seguir:*

1. Expanda o nó **Verificação por Demanda** na árvore do Console do Aplicativo.
2. No menu de contexto do nó filho **Verificação de Áreas Críticas**, selecione o comando **Iniciar**.

A tarefa é iniciada; o status da tarefa **Executando** é exibido na área de trabalho.

► *Para visualizar o log de tarefas,*

no painel de detalhes do nó **Verificação de Áreas Críticas.**, clique no link **Abrir log**.

Alteração do conjunto de componentes e recuperação do Kaspersky Embedded Systems Security 2.2

Os componentes do Kaspersky Embedded Systems Security 2.2 podem ser adicionados ou removidos. Você deve interromper a tarefa de Proteção de Arquivos em Tempo Real antes que possa remover o componente de Proteção de Arquivos em Tempo Real. Em outras circunstâncias, não há necessidade de interromper a tarefa de Proteção de Arquivos em Tempo Real ou o Kaspersky Security Service.

> Se o acesso do gerenciamento do aplicativo for protegido por senha, o Kaspersky Embedded Systems Security 2.2 solicitará a senha quando você tentar excluir ou modificar o conjunto de componentes na etapa adicional do Assistente de instalação.

► *Para modificar o conjunto de componentes do Kaspersky Embedded Systems Security 2.2:*

1. No menu **Iniciar**, selecione **Todos os programas > Kaspersky Embedded Systems Security 2.2 > Modificar ou Remover**.

   A janela **Modificar, reparar ou remover a instalação** do assistente de instalação é exibida.
2. Selecione **Modificar conjunto de componentes**. Clique no botão **Avançar**.

   A janela **Instalação personalizada** é exibida.
3. Na janela **Instalação personalizada**, na lista de componentes disponíveis, selecione os componentes que deseja adicionar ao Kaspersky Embedded Systems Security 2.2 ou que deseja remover. Para isso, execute as seguintes ações:
   - Para alterar o conjunto de componentes, clique no botão ao lado do nome do componente selecionado e, no menu de contexto, selecione:
     - **O componente será instalado no disco rígido local**, se você desejar instalar um componente;
     - **O componente e os seus subcomponentes serão instalados no disco rígido local**, se você desejar instalar um grupo de componentes.
   - Para remover componentes instalados anteriormente, clique no botão ao lado do nome do componente selecionado e, no menu de contexto, selecione **O componente não estará disponível**.

   Clique no botão **Instalar**.
4. Na janela **Pronto para instalar**, confirme a modificação do conjunto de componentes do software clicando no botão Instalar.
5. Na janela exibida quando a instalação for concluída, clique no botão **OK**.

O conjunto de componentes do Kaspersky Embedded Systems Security 2.2 será modificado com base nas configurações especificadas.

Se ocorrerem problemas na operação do Kaspersky Embedded Systems Security 2.2 (travamentos do Kaspersky Embedded Systems Security 2.2; as tarefas travam ou não iniciam), é possível tentar restaurar o Kaspersky Embedded Systems Security 2.2. Você pode executar uma restauração salvando as configurações atuais do Kaspersky Embedded Systems Security 2.2 ou pode selecionar uma opção para reinicializar todas as configurações do Kaspersky Embedded Systems Security 2.2 com os seus valores padrões.

► *Para recuperar o Kaspersky Embedded Systems Security 2.2 após o travamento do aplicativo ou de uma tarefa, siga as etapas a seguir:*

1. No menu **Iniciar**, selecione **Todos os programas > Kaspersky Embedded Systems Security 2.2 > Modificar ou Remover**.

   A janela **Modificar, reparar ou remover instalação** do Assistente de instalação é exibida.

2. Selecione **Reparar componentes instalados**. Clique no botão **Avançar**.

   Isso abre a janela **Reparar componentes instalados**.

3. Na janela **Reparar componentes instalados**, marque a caixa de seleção **Restaurar configurações recomendadas do aplicativo** se deseja reinicializar as configurações definidas do aplicativo e restaurar as configurações padrão do Kaspersky Embedded Systems Security 2.2. Clique no botão **Instalar**.
4. Na janela **Pronto para reparar**, confirme a operação de reparo clicando no botão **Instalar**.
5. Na janela exibida após a conclusão da operação de reparo, clique no botão **OK**.

O Kaspersky Embedded Systems Security 2.2 será restaurado com base nas configurações especificadas.

Desinstalação usando o Assistente de instalação

Esta seção contém instruções sobre a remoção do Kaspersky Embedded Systems Security 2.2 e do Console do Aplicativo de um computador protegido usando o Assistente de instalação.

Desinstalação do Kaspersky Embedded Systems Security 2.2

Os nomes de configurações podem variar em diferentes sistemas operacionais Windows.

O Kaspersky Embedded Systems Security 2.2 pode ser desinstalado do computador protegido usando o Assistente de configuração/desinstalação.

Pode ser necessária uma reinicialização após a desinstalação do Kaspersky Embedded Systems Security 2.2 de um computador protegido. A reinicialização poderá ser adiada.

A desinstalação, recuperação e instalação do aplicativo por meio do painel de controle do Windows não estarão disponíveis se o sistema operacional utilizar o recurso UAC (Controle de Conta de Usuário) ou o acesso ao aplicativo for protegido por senha.

Se o acesso do gerenciamento do aplicativo for protegido por senha, o Kaspersky Embedded Systems Security 2.2 solicitará a senha quando você tentar excluir ou modificar o conjunto de componentes na etapa adicional do Assistente de instalação.

► *Para desinstalar o Console do Kaspersky Embedded Systems Security 2.2:*

1. No menu **Iniciar**, selecione **Todos os programas > Kaspersky Embedded Systems Security 2.2 > Modificar ou Remover**.

   A janela **Modificar, reparar ou remover a instalação** do assistente de instalação é exibida.
2. Selecione **Remover componentes do software**. Clique no botão **Avançar**.

   A janela **Configurações avançadas de desinstalação do aplicativo** é exibida.
3. Se necessário, na janela **Configurações avançadas de desinstalação do aplicativo**:
   a. Marque a caixa de seleção **Exportar objetos da Quarentena** para que o Kaspersky Embedded Systems Security 2.2 exporte objetos que foram isolados em Quarentena. Esta caixa é desmarcada por padrão.
   b. Marque a caixa de seleção **Exportar objetos do Backup**, para exportar objetos do Backup do Kaspersky Embedded Systems Security 2.2. Esta caixa é desmarcada por padrão.
   c. Clique no botão **Salvar em** e selecione a pasta para onde deseja exportar objetos que estão sendo restaurados. Por padrão, os objetos serão exportados para %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security 2.2\Uninstall.

      Clique no botão **Avançar**.
4. Na janela **Pronto para desinstalar**, confirme a desinstalação clicando no botão **Desinstalar**.
5. Na janela exibida após a conclusão da desinstalação, clique no botão **OK**.

O Kaspersky Embedded Systems Security 2.2 será desinstalado de um computador protegido.

Desinstalação do Console do Kaspersky Embedded Systems Security 2.2

Os nomes de configurações podem variar em diferentes sistemas operacionais Windows.

Você pode desinstalar o Console do Aplicativo do computador usando o Assistente de configuração/desinstalação.

Após desinstalar o Console do Aplicativo, não é necessário reiniciar o computador.

► *Para desinstalar o Console do Aplicativo:*

1. No menu **Iniciar**, selecione **Todos os programas > Kaspersky Embedded Systems Security > Ferramentas de administração > Modificar ou Remover**.
2. A janela **Modificar, reparar ou remover** do assistente é exibida.

   Selecione **Remover componentes do software** e clique no botão **Avançar**.
3. A janela **Pronto para desinstalar** é exibida. Clique no botão **Remover**.

   A janela **Desinstalação concluída** é exibida.
4. Clique em **OK**.

A remoção está concluída e o Assistente de instalação é fechado.

Instalação e desinstalação do aplicativo a partir da linha de comando

Esta seção descreve as particularidades da instalação e desinstalação do Kaspersky Embedded Systems Security 2.2 a partir da linha de comando e contém exemplos de comandos para instalar e desinstalar o Kaspersky Embedded Systems Security 2.2 a partir da linha de comando e exemplos de comandos para adicionar e remover os componentes do Kaspersky Embedded Systems Security 2.2 a partir da linha de comando.

Nesta seção

Sobre a instalação e desinstalação do Kaspersky Embedded Systems Security 2.2 a partir da linha de comando

O Kaspersky Embedded Systems Security 2.2 pode ser instalado ou desinstalado e seus componentes adicionados ou removidos, executando os arquivos do pacote de instalação \product\ess_x86(x64).msi a partir da linha de comando após as configurações de instalação terem sido especificadas usando chaves.

O conjunto de “Ferramentas de administração” pode ser instalado no computador protegido ou em outro computador na rede para funcionar com o Console do Aplicativo local ou remotamente. Para isso, use o pacote de instalação \client\esstools.msi installation.

> Execute a instalação usando os direitos de uma conta incluída no grupo de administradores no computador onde o aplicativo foi instalado.

Se um dos arquivos \product\ess_x86 (x64) .msi for executado no computador protegido sem chaves adicionais, o Kaspersky Embedded Systems Security 2.2 será instalado com as configurações de instalação recomendadas.

O conjunto de componentes a ser instalado pode ser atribuído usando a opção de linha de comando ADDLOCAL listando os códigos dos componentes selecionados ou conjuntos de componentes.

Exemplos de comandos para instalar o Kaspersky Embedded Systems Security 2.2

Essa seção fornece exemplos de comandos usados para instalar o Kaspersky Embedded Systems Security 2.2.

> Em computadores executando uma versão de 32 bits do Microsoft Windows, execute os arquivos com o sufixo x86 no kit de distribuição. Em computadores executando uma versão de 64 bits do Microsoft Windows, execute os arquivos com o sufixo x64 no kit de distribuição.

Informações detalhadas sobre o uso dos comandos padrão do Windows Installer e as opções de linha de comando são fornecidas na documentação enviada pela Microsoft.

Exemplos de instalação do Kaspersky Embedded Systems Security 2.2 a partir do arquivo setup.exe

► *Para instalar o Kaspersky Embedded Systems Security 2.2 com as configurações de instalação recomendadas sem interação com o usuário, execute o seguinte comando:*

```
\product\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

► *Para instalar o Kaspersky Embedded Systems Security 2.2 com as seguintes configurações:*

- instale somente os componentes da Proteção de Arquivos em Tempo Real e de Verificação por Demanda;
- não execute a Proteção em Tempo Real ao iniciar o Kaspersky Embedded Systems Security 2.2;
- não exclua dos arquivos de verificação que a Microsoft Corporation recomenda a exclusão;

Execute o comando a seguir:

```
\product\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

Exemplos de comandos usados para a instalação: executando o arquivo .msi de um pacote de instalação

► *Para instalar o Kaspersky Embedded Systems Security 2.2 com as configurações de instalação recomendadas sem interação com o usuário, execute o seguinte comando:*

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

► *Para instalar o Kaspersky Embedded Systems Security 2.2 com as configurações de instalação recomendadas, visualize a interface da instalação e execute o seguinte comando:*

```
msiexec /i ess.msi /qf EULA=1 PRIVACYPOLICY=1
```

► *Para instalar o Kaspersky Embedded Systems Security 2.2 com a ativação usando o arquivo de chave C:\0000000A.key:*

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1
PRIVACYPOLICY=1
```

► *Para instalar o Kaspersky Embedded Systems Security 2.2 com uma verificação preliminar dos processos ativos e setores de inicialização dos discos locais, execute o seguinte comando:*

```
msiexec /i ess.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

► *Para instalar o Kaspersky Embedded Systems Security 2.2 salvando seus arquivos na pasta de destino C:\ESS, execute o comando a seguir:*

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

► *Para instalar o Kaspersky Embedded Systems Security 2.2: salve o arquivo de log da instalação com o nome ess.log na pasta onde o arquivo msi do pacote de instalação do Kaspersky Embedded Systems Security 2.2 está armazenado e execute o seguinte comando:*

```
msiexec /i ess.msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

► *Para instalar o Console do Kaspersky Embedded Systems Security 2.2, execute o seguinte comando:*

```
msiexec /i esstools.msi /qn EULA=1 PRIVACYPOLICY=1
```

► *Para instalar o Kaspersky Embedded Systems Security 2.2 com ativação usando o arquivo de chave C:\0000000A.key, configure o Kaspersky Embedded Systems Security 2.2 de acordo com as configurações descritas no arquivo de configuração C:\settings.xml e execute o seguinte comando:*

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

► *Para instalar o patch do aplicativo quando o Kaspersky Embedded Systems Security 2.2 for protegido por senha, execute o seguinte comando:*

```
msiexec /p "<msp file name with path>" UNLOCK_PASSWORD=<password>
```

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 2.2

O Kaspersky Embedded Systems Security 2.2 inicia as tarefas de proteção e verificação imediatamente após a instalação se o aplicativo tiver sido ativado. Se você selecionou **Ativar a proteção em tempo real após a instalação do aplicativo** durante a instalação do Kaspersky Embedded Systems Security 2.2, o aplicativo verifica objetos do sistema de arquivos do computador quando forem acessados. O Kaspersky Embedded Systems Security 2.2 executará a tarefa de Verificação de Áreas Críticas todas as sextas-feiras às 20h.

Recomendamos seguir as seguintes etapas após instalar o Kaspersky Embedded Systems Security 2.2:

- Iniciar a tarefa de atualização dos bancos de dados do Kaspersky Embedded Systems Security 2.2. Após a instalação, o Kaspersky Embedded Systems Security 2.2 verificará objetos usando o banco de dados incluído no respectivo kit de distribuição. Recomendamos atualizar o banco de dados do Kaspersky Embedded Systems Security 2.2 imediatamente. Para isso, você deve executar a tarefa de Atualização do Banco de Dados. O banco de dados será atualizado a cada hora de acordo com a programação padrão.

  Por exemplo, você pode executar a tarefa Atualização do banco de dados do aplicativo, executando o comando seguinte:

  KAVSHELL UPDATE /KL /PROXY:proxy.empresa.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456

  Nesse caso, as atualizações dos bancos de dados do Kaspersky Embedded Systems Security 2.2 são baixadas dos servidores de atualização da Kaspersky Lab. A conexão com a fonte de atualização é estabelecida por meio do servidor proxy (endereço do servidor proxy: proxy.company.com, porta: 8080) usando a autenticação NTLM incluída no Windows para acessar o servidor em uma conta (nome de usuário: inetuser; senha: 123456).

- Execute uma Verificação de Áreas Críticas no computador se nenhum software antivírus com a proteção de arquivo em tempo real estiver instalado no computador protegido antes de instalar o Kaspersky Embedded Systems Security 2.2.

► *Para iniciar a tarefa de Verificação de Áreas Críticas usando a linha de comando:*

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Esse comando salva o log de tarefas em um arquivo chamado scancritical.log incluído na pasta atual.

- Configure notificações do administrador sobre eventos do Kaspersky Embedded Systems Security 2.2.

Adicionar/remover componentes. Exemplos de comandos

O componente de Controle de Inicialização de Aplicativos é instalado automaticamente. Você não precisa especificá-lo na lista de valores de chave ADDLOCAL, adicionando ou excluindo os componentes do Kaspersky Embedded Systems Security 2.2.

► *Para adicionar o componente de Verificação por demanda aos componentes já instalados, execute o seguinte comando:*

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn
```

ou

```
\server\setup.exe /s /p "ADDLOCAL=Oas,Ods"
```

Se você enumerar os componentes que deseja instalar junto com os componentes já instalados, o Kaspersky Embedded Systems Security 2.2 reinstalará os componentes existentes.

► *Para remover os componentes instalados, execute o comando a seguir:*

```
msiexec /i ess.msi "ADDLOCAL=Oas,AppCntrl,Ksn,AntiExploit,DevCtrl,Firewall,
LogInspector,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVPro
tection,RamDisk REMOVE=Ods,Fim" /qn
```

Desinstalação do Kaspersky Embedded Systems Security 2.2. Exemplos de comandos

► *Para desinstalar o Kaspersky Embedded Systems Security 2.2 do computador protegido, execute o seguinte comando:*

```
msiexec /x ess.msi /qn
```

ou

- Para sistemas operacionais de 32 bits:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} /qn
```

- Para sistemas operacionais de 64 bits:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} /qn
```

► *Para desinstalar o Console do Kaspersky Embedded Systems Security 2.2, execute o seguinte comando:*

```
msiexec /x esstools.msi /qn
```

ou

- Para sistemas operacionais de 32 bits:

```
msiexec /x {A727008F-F8CC-4B35-848A-1AECEEF22178} /qn
```

- Para sistemas operacionais de 64 bits:

```
msiexec /x {D978C311-2D2D-41A3-8158-BDF97149CCD4} /qn
```

► *Para desinstalar o Kaspersky Embedded Systems Security 2.2 de um computador protegido em que a proteção por senha esteja ativa, execute o comando a seguir:*

- Para sistemas operacionais de 32 bits:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} UNLOCK_PASSWORD=*** /qn
```

- Para sistemas operacionais de 64 bits:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} UNLOCK_PASSWORD=*** /qn
```

Códigos de retorno

A tabela abaixo contém uma lista de códigos de retorno da linha de comando.

Tabela 13. Códigos de retorno

Código	Descrição
1324	O nome da pasta de destino contém caracteres inválidos.
25001	Direitos insuficientes para instalar o Kaspersky Embedded Systems Security 2.2. Para instalar o aplicativo, inicie o assistente de instalação com direitos de administrador local.
25003	O Kaspersky Embedded Systems Security 2.2 não pode ser instalado em computadores que executam essa versão do Microsoft Windows. Inicie o assistente de instalação paras versões de 64 bits do Microsoft Windows.
25004	Software incompatível detectado. Para continuar a instalação, desinstale o software a seguir: <lista de software incompatível>.
25010	O caminho indicado não pode ser utilizado para salvar objetos em quarentena.
25011	O nome da pasta para salvar objetos em quarentena contém caracteres inválidos.
26251	Não é possível fazer download de Contadores de desempenho DLL.
26252	Não é possível fazer download de Contadores de desempenho DLL.
27300	O driver não pode ser instalado.
27301	O driver não pode ser desinstalado.
27302	O componente de rede não pode ser instalado. O número máximo possível de dispositivos filtrados foi alcançado.
27303	Bancos de dados de antivírus não encontrados.

Instalação e desinstalação do aplicativo usando o Kaspersky Security Center

Esta seção contém informações gerais sobre a instalação do Kaspersky Embedded Systems Security 2.2 por meio do Kaspersky Security Center. Ela descreve também como instalar e desinstalar o Kaspersky Embedded Systems Security 2.2 por meio do Kaspersky Security Center e ações após a instalação do Kaspersky Embedded Systems Security 2.2.

Nesta seção

Informações gerais sobre a instalação por meio do Kaspersky Security Center

Você pode instalar o Kaspersky Embedded Systems Security 2.2 por meio do Kaspersky Security Center usando a tarefa de instalação remota.

Após a conclusão da tarefa de instalação remota, o Kaspersky Embedded Systems Security 2.2 será instalado com configurações idênticas em vários computadores.

Todos os computadores podem ser combinados em um único grupo de administração e uma tarefa de grupo criada para executar a instalação do Kaspersky Embedded Systems Security 2.2 nos computadores deste grupo.

Você pode criar uma tarefa para instalar remotamente o Kaspersky Embedded Systems Security 2.2 em um conjunto de computadores que não estão no mesmo grupo de administração. Ao criar essa tarefa, você deve gerar uma lista dos computadores individuais nos quais o Kaspersky Embedded Systems Security 2.2 deve ser instalado.

Informações detalhadas sobre a tarefa de instalação remota são fornecidas na *Ajuda do Kaspersky Security Center*.

Direitos para instalar ou desinstalar o Kaspersky Embedded Systems Security 2.2

A conta especificada na tarefa de instalação (remoção) remota deve estar incluída no grupo de administradores em cada um dos computadores protegidos em todos os casos exceto nos casos descritos abaixo:

- Se o Agente de Rede do Kaspersky Security Center já estiver instalado nos computadores nos quais o Kaspersky Embedded Systems Security 2.2 será instalado (qualquer que seja o domínio onde os computadores estão localizados e se eles pertencem a qualquer domínio).

  > Se o Agente de Rede ainda não estiver instalado nos computadores, você pode instalá-lo com o Kaspersky Embedded Systems Security 2.2 usando uma tarefa de instalação remota. Antes de instalar o Agente de Rede, certifique-se de que a conta que você deseja especificar na tarefa esteja incluída no grupo de administradores de cada um dos computadores.

- Todos os computadores nos quais você deseja instalar o Kaspersky Embedded Systems Security 2.2 estão no mesmo domínio do Servidor de Administração e o Servidor de Administração está registrado na conta **Admin do Domínio** (se essa conta tem direitos de administrador local nos computadores do domínio).

Por padrão, ao usar o método **Instalação forçada**, a tarefa de instalação remota é executada a partir da conta onde o Servidor de Administração é executado.

Ao trabalhar com tarefas de grupo ou com tarefas de conjuntos de computadores no modo de instalação forçada (desinstalação), uma conta deve ter os seguintes direitos em um computador cliente:

- Direito de executar aplicativos remotamente.
- Direitos ao recurso **Admin$**.
- Direito de **Fazer logon como um serviço**.

Procedimento de instalação do Kaspersky Embedded Systems Security 2.2 por meio do Kaspersky Security Center

> As informações detalhadas sobre a geração de um pacote de instalação e criação de uma tarefa de instalação remota são fornecidas no Manual de implementação do Kaspersky Security Center.

Se você pretende gerenciar o Kaspersky Embedded Systems Security 2.2 por meio do Kaspersky Security Center no futuro, certifique-se de que as seguintes condições sejam cumpridas:

- O computador em que o Servidor de Administração do Kaspersky Security Center está instalado também tem o Plug-in de Administração instalado (arquivo \product\klcfginst.exe no kit de distribuição do Kaspersky Embedded Systems Security 2.2).
- O Agente de Rede do Kaspersky Security Center está instalado nos computadores protegidos. Se o Agente de Rede do Kaspersky Security Center não estiver instalado nos computadores protegidos, você poderá instalá-lo junto com o Kaspersky Embedded Systems Security 2.2 usando uma tarefa de instalação remota.

Os computadores também podem ser combinados em um grupo de administração antecipadamente para que seja possível gerenciar as configurações de proteção usando políticas e tarefas de grupo do Kaspersky Security Center.

► *Para instalar o Kaspersky Embedded Systems Security 2.2 com a ajuda da tarefa de instalação remota, faça o seguinte:*

1. Inicialize do Console de Administração do Kaspersky Security Center.
2. No Kaspersky Security Center, expanda o nó **Instalação remota** e, no nó filho **Pacotes de Instalação**, selecione a opção **Criar pacote de instalação para um aplicativo da Kaspersky Lab**.
3. Insira o nome do pacote de instalação.
4. Especifique o arquivo ess.kud do kit de distribuição do Kaspersky Embedded Systems Security 2.2 como o arquivo do pacote de instalação.

   A janela **EULA e Política de Privacidade** é aberta.
5. Se você concordar com os termos e as condições do EULA e da Política de Privacidade, selecione as caixas **os termos e as condições deste EULA** e **Política de Privacidade descrevendo o manuseio de dados** para prosseguir com a instalação.

   > Você deve aceitar o Contrato de Licença e a Política de Privacidade para prosseguir.
6. Para alterar o conjunto de componentes do Kaspersky Embedded Systems Security 2.2 a ser instalado (consulte a seção "Alteração do conjunto de componentes e recuperação do Kaspersky Embedded Systems Security 2.2" na página 49) e as configurações de instalação padrão (consulte a seção "Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer" na página 30) no pacote de instalação:
   a. No Kaspersky Security Center, expanda o nó **Instalação remota**.
   b. Na área de trabalho do nó filho **Pacotes de instalação** abra o menu de contexto pacote de instalação do Kaspersky Embedded Systems 2.2 criado e selecione **Propriedades**.
   c. Na janela **Propriedades: <nome do pacote de instalação>** na seção **Configurações**, faça o seguinte:
      a. No grupo de configurações **Componentes a instalar**, marque as caixas de seleção junto dos nomes de componentes do Kaspersky Embedded Systems Security 2.2 que deseja instalar.
      b. Para poder indicar uma pasta de destino que não a pasta padrão, especifique o nome da pasta e o caminho no campo **Pasta de destino**.

         O caminho para a pasta de destino pode conter variáveis de ambiente do sistema. Se a pasta não existir no computador, ela será criada.
      c. No grupo **Configurações avançadas de instalação**, defina as seguintes configurações:
         - Verificar o computador quanto à existência de vírus antes da instalação.
         - Ativar a proteção em tempo real após a instalação do aplicativo.
         - Adicionar arquivos recomendados pela Microsoft à lista de exclusões.
      d. Adicionar arquivos recomendados da Kaspersky Lab à lista de exclusões.
   d. Na janela de diálogo **Propriedades: <nome do pacote de instalação>**, clique em **OK**.
7. No nó **Pacotes de instalação**, crie uma tarefa para instalar remotamente o Kaspersky Embedded Systems Security 2.2 nos computadores selecionados (grupo de administração). Defina as configurações da tarefa.

   Para obter mais informações sobre a criação e configuração de tarefas de instalação remotas, consulte a *Ajuda do Kaspersky Security Center*.
8. Execute a tarefa de instalação remota para o Kaspersky Embedded Systems Security 2.2.

O Kaspersky Embedded Systems Security 2.2 será instalado nos computadores especificados na tarefa.

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 2.2

Após o Kaspersky Embedded Systems Security 2.2 ser instalado, recomendamos que os bancos de dados do Kaspersky Embedded Systems Security 2.2 nos computadores sejam atualizados e que uma Verificação de Áreas Críticas dos computadores seja executada, se nenhum aplicativo de antivírus com a função Proteção em tempo real ativada tiver sido instalado nos computadores antes da instalação do Kaspersky Embedded Systems Security 2.2.

Se os computadores nos quais o Kaspersky Embedded Systems Security 2.2 foi instalado forem unificados em um único grupo de administração no Kaspersky Security Center, você pode executar estas tarefas usando os seguintes métodos:

1. Criar tarefas de Atualização do Banco de Dados para o grupo de computadores nos quais o Kaspersky Embedded Systems Security 2.2 foi instalado. Definir o Servidor de Administração do Kaspersky Security Center como a fonte de atualização.
2. Criar uma tarefa de grupo de Verificação por Demanda com o status de tarefa de Verificação de Áreas Críticas. O Kaspersky Security Center avalia o status de segurança de cada computador no grupo com base nos resultados da execução desta tarefa, não com base nos resultados da tarefa de Verificação de Áreas Críticas.
3. Criar uma nova política para o grupo de computadores. Nas propriedades da política criada, na guia **Tarefas do sistema**, desative o início programado de tarefas de verificação do sistema conforme necessário e das tarefas de atualização do banco de dados nos computadores do grupo de administração.

Você também pode configurar notificações de administrador sobre eventos do Kaspersky Embedded Systems Security 2.2.

Instalação do Console do Aplicativo por meio do Kaspersky Security Center

As informações detalhadas sobre a criação de um pacote de instalação e de uma tarefa de instalação remota são fornecidas no *Manual de Implementação do Kaspersky Security Center*.

► *Para instalar o Console do Aplicativo usando a tarefa de instalação remota:*

1. No Console de Administração do Kaspersky Security Center, expanda o nó **Instalação remota** e, no nó filho **Pacotes de Instalação**, crie um novo pacote de instalação na base do arquivo client\setup.exe. Ao criar um novo pacote de instalação:
   - Na janela **Selecionar o pacote de distribuição para instalação**, selecione o arquivo client\setup.exe na pasta do kit de distribuição do Kaspersky Embedded Systems Security 2.2 e marque a caixa de seleção **Copiar atualizações do repositório para o pacote de instalação**.
   - Se necessário, use a opção de linha de comando ADDLOCAL para modificar o conjunto de componentes a ser instalado no campo **Configurações de inicialização do arquivo executável** (opcional) e altere a pasta de destino.

     Por exemplo, para instalar o Console do Aplicativo de forma autônoma na pasta C:\KasperskyConsole sem instalar o arquivo de ajuda e a documentação, execute o seguinte comando:

     ```
     /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1
     PRIVACYPOLICY=1"
     ```

2. No nó **Pacotes de instalação**, crie uma tarefa para instalar remotamente o Console do Aplicativo nos computadores selecionados (grupo de administração). Defina as configurações da tarefa.

> Para obter mais informações sobre a criação e configuração de tarefas de instalação remotas, consulte a *Ajuda do Kaspersky Security Center*.

3. Execute a tarefa de instalação remota criada.

O Console do Aplicativo será instalado nos computadores especificados na tarefa.

Desinstalação do Kaspersky Embedded Systems Security 2.2 por meio do Kaspersky Security Center

> Se o acesso ao gerenciamento do Kaspersky Embedded Systems Security 2.2 em computadores da rede for protegido por senha, insira a senha ao criar uma tarefa de desinstalação de vários aplicativos. Se a proteção por senha não for gerenciada de modo centralizado pelo aplicativo, ele será desinstalado com êxito dos computadores protegidos por acesso nos quais a senha inserida corresponde ao valor definido. O Kaspersky Embedded Systems Security 2.2 não será desinstalado dos demais computadores.

► *Para desinstalar o Kaspersky Embedded Systems Security 2.2, execute os passos a seguir no Console de Administração do Kaspersky Security Center:*

1. No Console de Administração do Kaspersky Security Center, crie e inicie a tarefa de remoção do aplicativo.
2. Na tarefa, selecione o método de desinstalação (similar a selecionar o método de instalação; consulte a seção anterior) e especifique uma conta cujos direitos o Servidor de Administração irá usar para endereçar os computadores. Você pode desinstalar o Kaspersky Embedded Systems Security 2.2 apenas com configurações de desinstalação padrão (consulte a seção "Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer" na página 30).

Instalação e desinstalação via políticas de grupo do Active Directory

Esta seção descreve a instalação e desinstalação do Kaspersky Embedded Systems Security 2.2 via políticas de grupo do Active Directory. Ela também contém informações sobre ações após a instalação do Kaspersky Embedded Systems Security 2.2 via políticas de grupo.

Nesta seção

Instalação do Kaspersky Embedded Systems Security 2.2 via políticas de grupo do Active Directory

Você pode instalar o Kaspersky Embedded Systems Security 2.2 em vários computadores via políticas de grupo do Active Directory. Você pode instalar o Console do Aplicativo do mesmo modo.

Os computadores nos quais deseja instalar o Kaspersky Embedded Systems Security 2.2 ou o Console do Aplicativo devem estar em um único domínio e em uma única unidade organizada.

Os sistemas operacionais nos computadores nos quais deseja instalar o Kaspersky Embedded Systems Security 2.2 com a ajuda da política devem ser da mesma versão (32 ou 64 bits).

Você deve ter direitos de administrador do domínio.

Para instalar o Kaspersky Embedded Systems Security 2.2, use os pacotes de instalação ess_x86(x64).msi. Para instalar o Console do Aplicativo, use os pacotes de instalação esstools.msi.

> As informações detalhadas sobre o uso de políticas de grupo do Active Directory são fornecidas na documentação enviada pela Microsoft.

► *Para instalar o Kaspersky Embedded Systems Security 2.2 ou o Console do Aplicativo:*

1. Salve o arquivo msi do pacote de instalação que corresponde ao tamanho de palavra (32 ou 64 bits) da versão instalada do sistema operacional Microsoft Windows na pasta pública do controlador do domínio.
2. No controlador do domínio, crie uma nova política para o grupo ao qual os computadores pertencem.
3. Usando o **Editor de Objetos de Política de Grupo**, crie um novo pacote de instalação no nó **Configuração do Computador**. Especifique o caminho para o arquivo msi do pacote de instalação do Kaspersky Embedded Systems Security 2.2 (ou do Console do Aplicativo) em formato UNC (Universal Naming Convention).
4. Marque a caixa de seleção do Windows Installer **Instalar sempre com privilégios elevados** tanto no nó **Configuração do Computador** quanto no nó **Configuração do Usuário** do grupo selecionado.
5. Aplique as alterações com o comando `gpupdate / force`.

O Kaspersky Embedded Systems Security 2.2 será instalado no grupo dos computadores após o respetivo reinício e antes de fazer login no Microsoft Windows.

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 2.2

Após instalar o Kaspersky Embedded Systems Security 2.2 nos computadores protegidos, recomenda-se que você atualize imediatamente o banco de dados do aplicativo e execute uma Verificação de Áreas Críticas. Você pode executar estas ações (consulte a seção "Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 2.2" na página 46) do Console do Aplicativo.

Você também pode configurar notificações de administrador sobre eventos do Kaspersky Embedded Systems Security 2.2.

Desinstalação do Kaspersky Embedded Systems Security 2.2 via políticas de grupo do Active Directory

Se você instalou o Kaspersky Embedded Systems Security 2.2 (ou o Console do Aplicativo) nos computadores do grupo usando a política de grupo do Active Directory, você poderá usar esta política para desinstalar o Kaspersky Embedded Systems Security 2.2 (ou o Console do Aplicativo).

É possível desinstalar o aplicativo somente com os parâmetros de desinstalação padrão.

> As informações detalhadas sobre o uso de políticas de grupo do Active Directory são fornecidas na documentação enviada pela Microsoft.

> Se o acesso ao gerenciamento do aplicativo for protegido por senha, a desinstalação do Kaspersky Embedded Systems Security 2.2 usando as políticas de grupo do Active Directory não estará disponível.

► *Para desinstalar o Kaspersky Embedded Systems Security 2.2 ou o Console do Aplicativo:*

1. Selecione a unidade organizacional no controlador do domínio a partir dos computadores que deseja excluir o Kaspersky Embedded Systems Security 2.2 ou o Console do Aplicativo.
2. Selecione a política criada para a instalação do Kaspersky Embedded Systems Security 2.2 e no **Editor de Objeto de Políticas de Grupo**, no nó **Instalação de software** (**Configuração do Computador** >**Configuração de programa** > **Instalação de software**) abra o menu de contexto do pacote de instalação do Kaspersky Embedded Systems Security 2.2 (ou do Console do Aplicativo) e selecione o comando **Todas as tarefas > Remover**.
3. Selecione o método de remoção **Desinstalar o software imediatamente de usuários e computadores**.
4. Aplique as alterações com o comando `gpupdate / force`.

O Kaspersky Embedded Systems Security 2.2 é removido dos computadores após eles serem reiniciados e antes de fazer login no Microsoft Windows.

Verificação das funções do Kaspersky Embedded Systems Security 2.2 Uso do vírus de teste EICAR

Esta seção descreve o vírus de teste EICAR e como usá-lo para verificar os recursos de Proteção em Tempo Real e Verificação por Demanda do Kaspersky Embedded Systems Security 2.2.

Nesta seção

Sobre o vírus de teste EICAR

Esse vírus de teste é projetado para verificar a operação dos aplicativos de antivírus. Ele foi desenvolvido pelo European Institute for Computer Antivirus Research (EICAR).

> O vírus de teste não é um vírus e não contém um código de programa para o seu computador, mas a maioria dos aplicativos antivírus dos fornecedores identifica uma ameaça nele.

O arquivo que contém esse vírus de teste chama-se eicar.com. Você pode baixá-lo no site do EICAR http://www.eicar.org/anti_virus_test_file.htm.

> Antes de salvar o arquivo em uma pasta no disco rígido do computador, certifique-se de que a Proteção de Arquivos em Tempo Real nesse disco esteja desativada.

O arquivo eicar.com contém uma linha de texto. Ao verificar o arquivo, o Kaspersky Embedded Systems Security 2.2 detecta uma ameaça de teste nesta linha de texto, atribui o status **Infectado** e exclui o arquivo. As informações sobre a ameaça detectada no arquivo aparecerão no Console do Aplicativo e no log de tarefas.

Você pode usar o arquivo eicar.com para verificar como o Kaspersky Embedded Systems Security 2.2 desinfecta objetos infectados e como detecta objetos possivelmente infectados. Para fazer isso, abra o arquivo usando um editor de texto, adicione um dos prefixos listados na tabela abaixo ao início da linha de texto no arquivo e salve o arquivo com um novo nome, por exemplo, eicar_cure.com.

> Para certificar-se de que o Kaspersky Embedded Systems Security 2.2 processe o arquivo eicar.com com um prefixo, na seção de configurações de segurança **Proteção de objetos** defina o valor **Todos os objetos** para as tarefas de Proteção de Arquivos em Tempo Real e de Verificação por Demanda padrão do Kaspersky Embedded Systems Security 2.2.

Tabela 14. Prefixos em arquivos EICAR

Prefixo	Status do arquivo após a verificação e a ação do Kaspersky Embedded Systems Security 2.2
Nenhum prefixo	O Kaspersky Embedded Systems Security 2.2 atribui o status **Infectado** ao objeto e o exclui.
SUSP–	O Kaspersky Embedded Systems Security 2.2 atribui o status **Provavelmente infectado** ao objeto (detectado pelo analisador heurístico) e o exclui (objetos possivelmente infectados não são desinfectados).
WARN–	O Kaspersky Embedded Systems Security 2.2 atribui o status **Provavelmente infectado** ao objeto (o código do objeto corresponde em parte ao código de uma ameaça) e o exclui (objetos possivelmente infectados não são desinfectados).
CURE–	O Kaspersky Embedded Systems Security 2.2 atribui o status **Infectado** ao objeto e o desinfecta. Se a desinfecção for bem-sucedida, o texto inteiro no arquivo será substituído pela palavra "CURE".

Teste de Proteção em Tempo Real e Verificação por Demanda

Após instalar o Kaspersky Embedded Systems Security 2.2, você pode confirmar se o Kaspersky Embedded Systems Security 2.2 encontra objetos contendo códigos maliciosos. Para verificar, você pode usar um vírus de teste do EICAR (consulte a seção "Sobre o vírus de teste EICAR" na página 64).

► *Para verificar o recurso de Proteção em Tempo Real, siga estas etapas:*

1. Faça download do arquivo eicar.com do site do EICAR http://www.eicar.org/anti_virus_test_file.htm. Salve-o na pasta pública na unidade local de qualquer um dos computadores da rede.

   Antes de salvar o arquivo na pasta, certifique-se de que a Proteção de Arquivos em Tempo Real esteja desativada na pasta.

2. Se você desejar verificar o funcionamento das notificações de usuário da rede, certifique-se de que o Serviço Windows Messenger da Microsoft esteja ativado tanto no computador protegido quanto no computador onde você salvou o arquivo eicar.com.
3. Abrir o Console do Aplicativo.
4. Copie o arquivo eicar.com salvo na unidade local do computador protegido usando um dos seguintes métodos:
   - Para testar as notificações por meio da janela Serviços de Terminal, copie o arquivo eicar.com no computador após conectar ao computador usando o utilitário Remote Desktop Connection.
   - Para testar notificações por meio do Serviço Windows Messenger da Microsoft, use os locais da rede do computador para copiar o arquivo eicar.com do computador onde você o salvou.

A Proteção de Arquivos em Tempo Real funciona corretamente se as seguintes condições forem atendidas:

- O arquivo eicar.com foi excluído do computador protegido.
- No Console do Aplicativo, o log de tarefas recebeu o status de **Crítico**. Uma linha apareceu no log com informações sobre uma ameaça no arquivo eicar.com. (Para visualizar o log de tarefas, na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**, selecione a tarefa de Proteção de Arquivos em Tempo Real e, no painel de detalhes do nó, clique no link **Abrir log**).
  - Uma mensagem do Serviço Windows Messenger da Microsoft terá aparecido no computador de onde você copiou o arquivo, como se segue: `O Kaspersky Embedded Systems Security 2.2 bloqueou acesso ao <caminho do arquivo no computador>\eicar.com no computador <nome da rede do computador> às <hora em que o evento ocorreu>. Razão: Ameaça detectada. Vírus: EICAR-Test-File. Nome de usuário: <nome do usuário>. Nome do computador: <nome da rede do computador a partir da qual você copiou o arquivo>.`

  Certifique-se de que o Serviço Windows Messenger da Microsoft esteja funcionando no computador a partir do qual você copiou o arquivo eicar.com.

► *Para verificar o recurso de Verificação por Demanda, siga estas etapas:*

1. Baixe o arquivo eicar.com do site do EICAR http://www.eicar.org/anti_virus_test_file.htm. Salve-o na pasta pública na unidade local de qualquer um dos computadores da rede.

   Antes de salvar o arquivo na pasta, certifique-se de que a Proteção de Arquivos em Tempo Real esteja desativada na pasta.

2. Abra o Console do Aplicativo.
3. Faça o seguinte:
   a. Expanda o nó **Verificação por Demanda** na árvore do Console do Aplicativo.
   b. Selecione o nó filho **Verificação de Áreas Críticas**.
   c. Na guia **Configurações do escopo da verificação**, abra o menu de contexto no nó **Rede** e selecione **Adicionar arquivo de rede**.
   d. Insira o caminho de rede para o arquivo eicar.com no computador remoto no formato UNC (Universal Naming Convention).
   e. Marque a caixa de seleção para incluir o caminho de rede adicionado ao escopo da verificação.
   f. Execute a tarefa de Verificação de áreas críticas.

A Verificação por Demanda funcionará da maneira correta se as seguintes condições forem atendidas:

- O arquivo eicar.com foi excluído da unidade de disco rígido do computador.
- No Console do Aplicativo, o log de tarefas recebeu o status de **Crítico**; no log de execução da tarefa de Verificação de Áreas Críticas apareceu uma linha com informações sobre uma ameaça no arquivo eicar.com. (Para visualizar o log de tarefas, na árvore do Console do Aplicativo, expanda o nó filho **Verificação por Demanda**, selecione a tarefa Verificação de Áreas Críticas e, no painel de detalhes, clique no link **Abrir log**).

Interface do aplicativo

Você pode controlar o Kaspersky Embedded Systems Security 2.2 pelo Console do Aplicativo local e o Plug-in de Administração. As ações com o Console do Aplicativo local são descritas no *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*. A interface do Console de Administração do Kaspersky Security Center é usada para executar ações com o Plug-in de Administração. Consulte informações detalhadas sobre a interface do Kaspersky Security Center na *Ajuda do Kaspersky Security Center*.

Licenciamento do aplicativo

Esta seção fornece informações sobre os principais conceitos relacionados ao licenciamento do aplicativo.

Neste capítulo

Sobre o Contrato de Licença do Usuário Final

O *Contrato de Licença do Usuário Final* é um contrato vinculativo entre o usuário e a AO Kaspersky Lab, que estipula os termos em que poderá usar o aplicativo.

Leia com atenção os termos do Contrato de Licença do Usuário Final antes de começar a usar o aplicativo.

Você pode rever os termos do Contrato de Licença do Usuário Final de várias formas:

- Durante a instalação do Kaspersky Embedded Systems Security 2.2
- Abrindo e lendo o arquivo license.txt. Esse documento é incluído no kit de distribuição do aplicativo

Ao confirmar que você aceita o Contrato de Licença do Usuário Final ao instalar o aplicativo, isso significa que você aceita e concorda com os termos do Contrato de Licença do Usuário Final. Se você não aceitar os termos do Contrato de Licença do Usuário Final, você deve cancelar a instalação do aplicativo e não usar o aplicativo.

Sobre a licença

Uma licença é um direito por tempo limitado de usar o aplicativo, concedido a você ao abrigo do Contrato de Licença do Usuário Final.

Uma licença válida dá a você o direito de receber os serviços seguintes:

- O uso do aplicativo de acordo com os termos do Contrato de Licença do Usuário Final
- Suporte técnico

O escopo do serviço e o termo do uso do aplicativo dependem do tipo de licença com que o aplicativo foi ativado.

O aplicativo é ativado usando um arquivo de chave para uma licença comercial adquirida.

Uma licença comercial é uma licença paga concedida após a compra do aplicativo.

O Kaspersky Embedded Systems Security 2.2 oferece dois tipos de licenças comerciais:

- Licença padrão do Kaspersky Embedded Systems Security
- A licença estendida do Kaspersky Embedded Systems Security Compliance Edition, que inclui dois componentes de inspeção do sistema adicionais: Monitor de Integridade de Arquivos e Inspeção do Log.

Quando a licença comercial expira, o aplicativo continua funcionando, mas alguns recursos se tornam inacessíveis (por exemplo, os bancos de dados do Kaspersky Embedded Systems Security 2.2 não podem ser atualizados). Para continuar usando todos os recursos do Kaspersky Embedded Systems Security 2.2, você deve renovar sua licença comercial.

Para garantir proteção máxima contra ameaças à segurança do seu computador, é recomendado renovar a licença antes que ela expire.

Certifique-se de que a chave adicional que você adiciona tem uma data de expiração posterior à da chave ativa.

Sobre o certificado da licença

Um *certificado da licença* é um documento fornecido a você junto com um arquivo de chave ou código de ativação (se aplicável).

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

- Número de ordem
- Informações sobre o usuário a quem foi concedida a licença
- Informações sobre o aplicativo que pode ser ativado com a licença fornecida
- Limite do número de unidades de licenciamento (p. ex., dispositivos nos quais o aplicativo pode ser usado de acordo com a licença fornecida)
- Data inicial da validade da licença
- Data de expiração da licença ou período da licença
- Tipo de licença

Sobre o código de ativação

Um *código de ativação* é uma sequência única de 20 letras e números. Você deve inserir um código de ativação para adicionar uma chave para ativar o Kaspersky Embedded Systems Security 2.2. Você recebe o código de ativação no endereço de e-mail que forneceu ao adquirir o Kaspersky Embedded Systems Security 2.2.

Para ativar o aplicativo com um código de ativação, é preciso ter acesso à Internet para se conectar aos servidores de ativação da Kaspersky Lab.

Se você perdeu seu código de ativação após instalar o aplicativo, ele pode ser recuperado. Você pode precisar do código de ativação para registrar um Kaspersky CompanyAccount, por exemplo. Para recuperar seu código de ativação, entre em contato com o Suporte Técnico da Kaspersky Lab.

Sobre a chave

Uma *chave* é uma sequência de bits com a qual você pode ativar e subsequentemente usar o aplicativo de acordo com os termos do Contrato de Licença do Usuário Final. Uma chave é criada pela Kaspersky Lab.

Você pode adicionar a chave ao aplicativo usando um arquivo de chave. Após adicionar uma chave ao aplicativo, a chave é exibida na interface do aplicativo como uma sequência alfanumérica exclusiva.

A Kaspersky Lab pode colocar na lista negra uma chave por violações do Contrato de Licença. Se sua chave estiver bloqueada, uma chave diferente deve ser adicionada para o aplicativo trabalhar.

Uma chave pode ser uma "chave ativa" ou uma "chave adicional".

Uma chave *ativa* é a chave que o aplicativo usa atualmente para funcionar. Uma chave para uma licença comercial pode ser adicionada como chave ativa. O aplicativo não pode ter mais de uma chave ativa.

Uma *chave adicional* é uma chave que confirma o direito de usar o aplicativo mas que não se encontra atualmente em uso. Uma chave adicional torna-se ativa automaticamente quando a licença associada com a chave ativa atual expira. Uma chave adicional pode ser adicionada somente se houver uma chave ativa.

Sobre arquivo de chave

Um *arquivo de chave* é um arquivo com a extensão .key que você recebe da Kaspersky Lab. Os arquivos de chave destinam-se a ativar o aplicativo adicionando uma chave.

Você recebe um arquivo de chave no endereço de e-mail que forneceu quando adquiriu o Kaspersky Embedded Systems Security 2.2.

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

Você pode recuperar um arquivo de chave se ele for acidentalmente excluído. Você poderá precisar de um arquivo de chave para se registrar no Kaspersky CompanyAccount.

Para recuperar um arquivo de chave, é necessário executar uma das seguintes ações:

- Contatar o Suporte Técnico https://support.kaspersky.com.br/.
- Obtenha um arquivo de chave no site da Kaspersky Lab com base no código de ativação existente.

Sobre a coleta de dados

O Contrato de Licença do Kaspersky Embedded Systems Security 2.2, especificamente a seção intitulada “Termos do processamento de dados”, especifica os termos, a responsabilidade e o procedimento para enviar e processar os dados indicados neste Manual. Antes de aceitar o Contrato de Licença, revise cuidadosamente os seus termos bem como todos os documentos referenciados em links no Contrato de Licença.

Os dados que a Kaspersky Lab recebe de você durante o uso do aplicativo são protegidos e processados conforme a Política de Privacidade disponível em http://www.kaspersky.com/products-and-services-privacy-policy.

Ao aceitar os termos do Contrato de Licença, você aceita enviar automaticamente os seguintes dados à Kaspersky Lab:

- Para apoiar o mecanismo de recepção de atualizações – informações sobre o aplicativo instalado e a sua ativação: o identificador do aplicativo a ser instalado e a sua versão completa, inclusive o número da compilação, tipo e identificador da licença, o identificador de instalação, o identificador de tarefa de atualização exclusivo.
- Para usar a capacidade de navegar pelos artigos da Base de Dados de Conhecimento quando ocorrerem erros no aplicativo (serviço Redirecionador) – informações sobre o aplicativo e tipo de link, especificamente: o nome, localidade, e número da versão completa do aplicativo, tipo de link redirecionador e o identificador de erro.
- Para gerenciar confirmações para o processamento de dados – informações sobre o status da aceitação de contratos de licença e outros documentos que estipulam termos de transferência de dados: o identificador e a versão do Contrato de Licença ou outro documento, como parte do qual os termos de processamento de dados são aceitos ou recusados; um atributo, significando a ação do usuário (confirmação ou revogação da aceitação dos termos); data e hora de modificações de status da aceitação dos termos de processamento de dados.

Você pode rever os termos do Contrato de Licença do Usuário Final de várias formas:

- Durante a instalação do aplicativo, o Assistente de instalação do Kaspersky Embedded Systems Security 2.2 exibe o texto completo do Contrato de Licença na etapa de solicitação de aceitação dos termos do Contrato de Licença.
- A qualquer momento no arquivo TXT (license.txt) que contém o texto completo do Contrato de Licença. O arquivo está incluído no kit de distribuição do Kaspersky Embedded Systems Security 2.2 junto aos arquivos de instalação do aplicativo.

Processamento local de dados

Enquanto executa as funções principais do aplicativo descritas neste Manual, o Kaspersky Embedded Systems Security 2.2 processa e armazena localmente uma sequência de tipos de dados no computador protegido:

- Informações sobre arquivos verificados e objetos detectados, por exemplo, nomes e atributos de arquivos processados e caminhos completos deles na mídia verificada, ações realizadas nos arquivos verificados, contas de usuários que executam qualquer ação na rede protegida ou no computador protegido, nomes e dados sobre dispositivos verificados, informações sobre processos executados no sistema.
- Informações sobre atividades e configurações do sistema operacional, por exemplo, configurações do Firewall do Windows, entradas de Log de Eventos do Windows, nomes de contas de usuário, inicialização de arquivos executáveis, suas somas de verificação e seus atributos.

O Kaspersky Embedded Systems Security 2.2 processa e armazena dados como parte da funcionalidade básica do aplicativo, em particular para registrar em log eventos do aplicativo e receber dados de diagnósticos. Os dados processados localmente são protegidos conforme as configurações definidas e aplicadas do aplicativo.

O Kaspersky Embedded Systems Security 2.2 permite configurar o nível da proteção dos dados processados localmente: você pode alterar privilégios de usuários relativos a acesso de dados de processo, alterar o período de retenção de dados para tais dados, desativar inteira ou parcialmente a funcionalidade que envolve o registo de dados e alterar o caminho e os atributos da pasta na mídia em que os dados são registrados em log.

Informações detalhadas sobre a configuração da funcionalidade do aplicativo que relativa ao processamento de dados e as configurações padrão do armazenamento de dados processados podem ser encontradas nas seções correspondentes deste Manual.

Por padrão, todos os dados armazenados em um computador local são removidos após a desinstalação do Kaspersky Embedded Systems Security 2.2, exceto os arquivos com informações de diagnóstico (arquivos de rastreamento e despejo) e também os registros de atividade do aplicativo do Log de Eventos do Windows. Você precisa remover manualmente estes arquivos. Você pode encontrar a informações detalhadas sobre a configuração de processos de diagnóstico nas seções correspondentes deste Manual.

Ao desinstalar o aplicativo, você pode salvar o conteúdo de armazenamentos de backup e de quarentena.

Ativar aplicativo com chave

Você pode ativar o Kaspersky Embedded Systems Security 2.2 aplicando uma chave.

Se um arquivo de chave já tiver sido adicionado ao Kaspersky Embedded Systems Security 2.2 e você adicionar outra chave como chave ativa, a nova chave substitui a chave adicionada anteriormente. A chave ativa instalada anteriormente é removida.

Se uma chave adicional já tiver sido adicionada ao Kaspersky Embedded Systems Security 2.2 e você adicionar outra chave como chave adicional, a nova chave substitui a chave adicionada anteriormente. A chave adicional instalada anteriormente é removida.

Se uma chave ativa e uma chave adicional já tiverem sido adicionadas ao Kaspersky Embedded Systems Security 2.2 e você adicionar uma nova chave como chave ativa, a nova chave substitui a chave ativa adicionada anteriormente; a chave adicional não é excluída.

► *Para ativar o Kaspersky Embedded Systems Security 2.2:*

1. Na árvore do Console do Aplicativo, expanda o nó **Licenciamento**.
2. No painel de detalhes do nó **Licenciamento**, clique no link **Adicionar chave**.
3. Na janela exibida, clique no botão **Procurar** e selecione um arquivo de chave com a extensão .key.

   > Você também pode adicionar uma chave como adicional. Para adicionar uma chave adicional, selecione a caixa de verificação **Usar como chave adicional**.

4. Clique em **OK**.

A chave selecionada será aplicada. As informações sobre a chave adicionada estarão disponíveis no nó **Licenciamento**.

Visualizando informações sobre a licença atual

Visualizando informações de licenciamento

As informações sobre a licença atual são exibidas no painel de detalhes do nó **Kaspersky Embedded Systems Security** do Console do Aplicativo. O status da chave pode ter os seguintes valores:

- **Verificando o status da chave** – o Kaspersky Embedded Systems Security 2.2 está verificando o arquivo de chave adicionado ou o código de ativação aplicado e aguardando uma resposta sobre o status da chave atual.
- **Data de expiração da licença** – o Kaspersky Embedded Systems Security 2.2 foi ativado até a data e hora especificadas. O status da chave é realçado em amarelo nos seguintes casos:
  - A licença expirará em 14 dias e nenhuma chave adicional ou código de ativação foi adicionado.
  - A chave adicionada foi colocada na lista negra e está prestes a ser bloqueada.
- **Aplicativo não ativado** – o Kaspersky Embedded Systems Security 2.2 não está ativado porque a chave não foi adicionada ou o código de ativação não foi aplicado. O status é realçado em vermelho.
- **Licença expirou** – o Kaspersky Embedded Systems Security 2.2 não está ativado porque a licença expirou. O status é realçado em vermelho.
- **O Contrato de Licença do Usuário Final foi violado** – o Kaspersky Embedded Systems Security 2.2 é não ativado porque os termos do Contrato de Licença do Usuário Final (consulte a seção "Sobre o Contrato de Licença do Usuário Final" na página 67) foram violados. O status é realçado em vermelho.
- **A chave está na lista negra** – o arquivo de chave adicionado foi bloqueado e colocado na lista negra pela Kaspersky Lab, por exemplo, se a chave foi usada por terceiros para ativar o aplicativo ilegalmente. O status é realçado em vermelho.

Visualizando informações sobre a licença atual

► *Para visualizar as informações sobre a licença atual,*

Na árvore do Console do Aplicativo, expanda o nó **Licenciamento**.

As informações gerais sobre a licença atual são exibidas no painel de detalhes do nó **Licenciamento** (consulte a tabela abaixo).

Tabela 15. Informações gerais sobre a licença no nó Licenciamento

Campo	Descrição
Código de ativação	Número do código de ativação. Este campo é preenchido se você ativar o aplicativo usando um código de ativação.
Status da ativação	Informações sobre o status da ativação do aplicativo. As informações na coluna Status da ativação no painel de controle do nó Licenciamento podem ter os seguintes valores: • **Aplicado** – se você ativou o aplicativo usando um código de ativação ou chave. • **Ativação** – se você aplicou um código de ativação para ativar o aplicativo, mas o processo de ativação ainda não foi finalizado. O valor do status é alterado para Aplicado após a ativação do aplicativo ter sido concluída e os conteúdos do painel de detalhes do nó terem sido atualizados. • **Erro de ativação** – se a ativação do aplicativo falhou. Você pode visualizar a causa da ativação malsucedida no log de tarefas.
Chave	O número da chave que você usou para ativar o aplicativo.

Campo	Descrição
Tipo de licença	Tipo de licença: comercial.
Data de expiração	Data e hora de expiração da licença associadas à chave ativa.
Status do código de ativação ou da chave	Status do código de ativação ou status da chave: Ativo ou Adicional.

► *Para visualizar informações detalhadas sobre a licença,*

Selecione o nó **Licenciamento**, abra o menu de contexto na cadeia de caracteres com os dados de licença que deseja expandir e selecione **Propriedades**. Na janela **Propriedades: <Status do código de ativação ou status da chave>**, a guia **Geral** exibe informações detalhadas sobre a licença atual, e a guia **Avançado** exibe informações sobre o cliente e os detalhes de contato da Kaspersky Lab ou do revendedor onde você adquiriu o Kaspersky Embedded Systems Security 2.2 (consulte a tabela abaixo).

Tabela 16. Informações detalhadas de licença nas Propriedades: janela <Status de Código de ativação ou status da chave>

Campo	Descrição
Guia Geral	
Chave	O número da chave que você usou para ativar o aplicativo.
Data de adição da chave	Data em que a chave foi adicionada ao aplicativo.
Tipo de licença	Tipo de licença: comercial.
Dias até a expiração	Número de dias restantes até à expiração da licença associada à chave ativa.
Data de expiração	Data e hora de expiração da licença associadas à chave ativa. Se você ativar o aplicativo com uma assinatura ilimitada, o valor do campo é *Ilimitado*. Se o Kaspersky Embedded Systems Security 2.2 for incapaz de determinar a data de expiração da licença, o valor do campo é estabelecido como *Desconhecido*.
Aplicativo	O nome do aplicativo que foi ativado com a chave ou um código de ativação adicionado.
Restrição de uso da chave	Restrição de uso da chave (caso exista).
Elegível para suporte técnico	Informações se a Kaspersky Lab ou um de seus parceiros fornecerá suporte técnico para os clientes de acordo com os termos da licença.
Guia Adicional	
Informações sobre a licença	Número e tipo da licença atual.
Informações de suporte	Detalhes de contato da Kaspersky Lab ou de seu parceiro que está fornecendo o suporte técnico. Este campo pode ficar vazio se o suporte técnico não for fornecido.
Informações do proprietário	Informações sobre o cliente da licença: um nome do cliente e o nome de uma organização para a qual a licença foi adquirida.

Limitações funcionais na expiração da licença

Quando a licença atual expirar, as seguintes limitações na operação dos componentes funcionais serão aplicadas:

- Todas as tarefas serão interrompidas, exceto as tarefas de Proteção de Arquivos em Tempo Real, Verificação por Demanda e Controle de Integridade de Aplicativos.
- A inicialização de qualquer tarefa, exceto a Proteção em Tempo Real, Verificação por Demanda e Controle de Integridade de Aplicativos, será negada. Essas tarefas continuam a ser executadas usando os bancos de dados de antivírus antigos.
- A funcionalidade de Prevenção de Exploits será limitada:
  - Os processos serão protegidos até que sejam reiniciados.
  - Os novos processos não podem ser adicionados ao escopo da proteção.

Outras funções (armazenamento, logs, informações de diagnóstico) ainda estarão disponíveis.

Renovação da licença

Por padrão, quando faltam 14 dias para a expiração da licença, o Kaspersky Embedded Systems Security 2.2 notifica o usuário. Nesse caso o status **Data de expiração da licença** no painel de detalhes do nó **Kaspersky Embedded Systems Security** é realçado em amarelo.

Você pode renovar a data de expiração da licença antes que ela termine usando uma chave ou um código de ativação adicional. Isso garante que seu servidor permaneça protegido após a expiração da licença existente e antes que você ative o aplicativo com uma nova licença.

► *Para renovar uma licença, siga as seguintes etapas:*

1. Compre um novo código de ativação ou um arquivo de chave.
2. Na árvore do Console do Aplicativo, abra o nó **Licenciamento**.
3. Execute uma das seguintes ações no painel de detalhes do nó **Licenciamento**:
   - Se deseja renovar uma licença usando uma chave adicional:
     a. Clique no link **Adicionar** chave.
     b. Na janela exibida, clique no botão **Procurar** e selecione um novo arquivo de chave com a extensão .key.
     c. Marque a caixa de seleção **Usar como chave adicional**.
   - Se deseja renovar uma licença usando um código de ativação:
     a. Clique no link **Adicionar código de ativação**.
     b. Insira o código de ativação comprado na janela exibida.
     c. Marque a caixa de seleção **Usar como chave adicional**.

   É necessária uma conexão com a Internet para aplicar um código de ativação.
4. Clique em **OK**.

A chave ou o código de ativação adicional serão adicionados e automaticamente aplicados após a expiração da licença atual do Kaspersky Embedded Systems Security 2.2.

Exclusão da chave

Você pode remover a chave adicionada.

Se uma chave adicional tiver sido adicionada ao Kaspersky Embedded Systems Security 2.2 e você remover a chave ativa, a chave adicional torna-se automaticamente a chave ativa.

Se você excluir uma chave adicionada, você pode restaurá-la aplicando novamente o arquivo de chave.

► *Para remover uma chave adicionada:*

1. Na árvore do Console do Aplicativo, selecione o nó **Licenciamento**.
2. No painel de detalhes do nó **Licenciamento**, na tabela contendo informações sobre chaves adicionadas, selecione a chave que deseja remover.
3. No menu de contexto da linha contendo informações sobre a chave selecionada, selecione **Remover**.
4. Clique no botão **Sim** na janela de confirmação para confirmar que você deseja excluir a chave.

A chave selecionada será removida.

Inicialização e interrupção do Plug-in do Kaspersky Embedded Systems Security 2.2

Esta seção contém informações sobre como inicializar e interromper o Plug-in de Administração do Kaspersky Embedded Systems Security 2.2 e o Kaspersky Security Service.

Neste capítulo

Iniciando o Plug-in de Administração do Kaspersky Embedded Systems Security 2.2

Nenhuma ação adicional é necessária para iniciar o Plug-in de Administração do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center. Depois que o Plug-in for instalado no computador do administrador, ele é iniciado simultaneamente com o Kaspersky Security Center. Informações detalhadas sobre a inicialização do Kaspersky Security Center podem ser encontradas na *Ajuda do Kaspersky Security Center*.

Inicialização e interrupção do Kaspersky Security Service

Por padrão, o Kaspersky Security Service é iniciado automaticamente no momento da inicialização do sistema operacional. O Kaspersky Security Service gerencia os processos de trabalho nos quais as tarefas de Proteção do Computador em Tempo Real, Controle de Atividades Locais, Verificação por Demanda e Atualização são executadas.

Por padrão, quando o Kaspersky Embedded Systems Security 2.2 é iniciado, as tarefas de Proteção de Arquivos em Tempo Real e Verificação na Inicialização do Sistema Operacional são iniciadas, bem como outras tarefas que estejam programadas para iniciar **Ao iniciar o aplicativo**.

Se o Kaspersky Security Service for interrompido, todas as tarefas em execução serão interrompidas. Após reiniciar o Kaspersky Security Service, o aplicativo inicia automaticamente apenas as tarefas cuja programação tem uma frequência de inicialização definida como **Ao iniciar o aplicativo**, enquanto as outras tarefas devem ser iniciadas manualmente.

Você pode iniciar e interromper o Kaspersky Security Service usando o menu de contexto do nó do **Kaspersky Embedded Systems Security** ou usando o snap-in do Microsoft Windows **Services**.

Você pode iniciar e interromper o aplicativo se for membro do grupo de Administradores no computador protegido.

► *Para interromper ou iniciar o aplicativo usando o Console do Aplicativo, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.
2. Selecione um dos seguintes itens:
   - **Parar o serviço**
   - **Iniciar o serviço**

O Kaspersky Security Service será iniciado ou interrompido.

Permissões de acesso para funções do Kaspersky Embedded Systems Security 2.2

Esta seção contém informações sobre permissões para gerenciar o Kaspersky Embedded Systems Security 2.2 e os serviços Windows registrados pelo aplicativo, bem como instruções sobre como configurar essas permissões.

Neste capítulo

Sobre permissões para gerenciar o Kaspersky Embedded Systems Security 2.2

Por padrão, o acesso a todas as funções do Kaspersky Embedded Systems Security 2.2 é concedido aos usuários do grupo Administradores no computador protegido, aos usuários do grupo Administradores de ESS criado no computador protegido durante a instalação do Kaspersky Embedded Systems Security 2.2, bem como ao grupo de sistema SYSTEM.

Os usuários com acesso à função **Editar** permissões do Kaspersky Embedded Systems Security 2.2 podem conceder acesso às funções do Kaspersky Embedded Systems Security 2.2 a outros usuários registrados no computador protegido ou incluídos no domínio.

Os usuários que não estiverem registrados na lista de usuários do Kaspersky Embedded Systems Security 2.2 não poderão abrir o Console do Aplicativo.

Você pode escolher um dos seguintes níveis predefinidos de acesso do Kaspersky Embedded Systems Security 2.2 para um usuário ou grupo de usuários:

- **Controle total** – acesso a todas as funções do aplicativo: capacidade de visualizar e editar configurações gerais do Kaspersky Embedded Systems Security 2.2, configurações de componentes, permissões de usuários do Kaspersky Embedded Systems Security 2.2 e também de visualizar estatísticas do Kaspersky Embedded Systems Security 2.2.
- **Editar** – acesso a todas as funções do aplicativo, exceto a edição das permissões de usuário: capacidade de visualizar e editar as configurações gerais do Kaspersky Embedded Systems Security 2.2 e do seu componente.
- **Ler** – capacidade de visualizar as configurações gerais, configurações de componentes, estatísticas e permissões de usuário do Kaspersky Embedded Systems Security 2.2.

Você também pode configurar permissões de acesso avançado (consulte a seção "Configurar permissões de acesso para o Kaspersky Embedded Systems Security 2.2 e Kaspersky Security Service" na página 83): permitir ou bloquear acesso a funções específicas do Kaspersky Embedded Systems Security 2.2.

Se você tiver configurado manualmente as permissões de acesso para um usuário ou grupo, o nível de acesso **Permissões especiais** será definido para este usuário ou grupo.

Tabela 17. Sobre permissões de acesso para funções do Kaspersky Embedded Systems Security 2.2

Direitos de usuário	Descrição
Gerenciamento de tarefas	Capacidade para iniciar/interromper/pausar/reiniciar tarefas do Kaspersky Embedded Systems Security 2.2.
Criação e exclusão de tarefas de Verificação por Demanda	Capacidade para criar e excluir tarefas de Verificação por Demanda.
Editar configurações	Capacidade para: • Importar as configurações do Kaspersky Embedded Systems Security 2.2 a partir de um arquivo de configuração. • Editar as configurações do aplicativo.
Configurações de leitura	Capacidade para: • Exibir as configurações gerais do Kaspersky Embedded Systems Security 2.2 e as configurações da tarefa. • Exportar as configurações do Kaspersky Embedded Systems Security 2.2 para o arquivo de configuração. • Exibir configurações para logs de tarefas, log de auditoria do sistema e notificações.
Gerenciar armazenamentos	Capacidade para: • Colocar objetos na Quarentena. • Remover objetos da Quarentena e do Backup. • Restaurar objetos da Quarentena e do Backup.
Gerenciar logs	Capacidade para excluir logs de tarefas e limpar o log de auditoria do sistema.
Ler logs	Capacidade para visualizar eventos do Antivírus em logs de tarefas e no log de auditoria do sistema.
Ler estatísticas	Capacidade para visualizar as estatísticas de cada tarefa do Kaspersky Embedded Systems Security 2.2.
Licenciamento do aplicativo	O Kaspersky Embedded Systems Security 2.2 pode ser ativado ou desativado.
Desinstalar o aplicativo	Capacidade para desinstalar o Kaspersky Embedded Systems Security 2.2.
Permissões de leitura	Capacidade para visualizar a lista de usuários do Kaspersky Embedded Systems Security 2.2 e privilégios de acesso de cada usuário.

Direitos de usuário	Descrição
Permissões de edição	Capacidade para: • Editar a lista de usuários com acesso ao gerenciamento de aplicativos. • Editar permissões de acesso do usuário às funções do Kaspersky Embedded Systems Security 2.2.

Sobre permissões para gerenciar o Kaspersky Security Service

Durante a instalação, o Kaspersky Embedded Systems Security 2.2 registra o Kaspersky Security Service (KAVFS) no Windows e ativa internamente componentes funcionais iniciados durante a inicialização do sistema operacional. Para reduzir o risco de acesso de terceiros às funções do aplicativo e configurações de segurança no computador protegido por meio do gerenciamento do Kaspersky Security Service, você pode restringir as permissões para gerenciar o Kaspersky Security Service a partir do Console do Aplicativo ou do Plug-in de Administração.

Por padrão, as permissões de acesso para gerenciar o Kaspersky Security Service são concedidas a usuários no grupo de "Administradores" no computador protegido, bem como aos grupos SERVICE e INTERACTIVE com permissões de leitura e ao grupo SYSTEM com permissões de leitura e execução.

Não é possível excluir a conta de usuário SYSTEM ou editar permissões para esta conta. Se as permissões da conta de usuário SYSTEM foram editadas, os privilégios máximos são restaurados para esta conta ao salvar as alterações.

Os usuários com acesso ao nível de função Editar permissões (consulte a seção "Sobre permissões para gerenciar o Kaspersky Embedded Systems Security 2.2" na página 78) podem conceder permissões de acesso para gerenciar o Kaspersky Security Service para outros usuários registrados no computador protegido ou incluídos no domínio.

Você pode selecionar um dos seguintes níveis predefinidos de permissões de acesso para um usuário ou grupo de usuários do Kaspersky Embedded Systems Security 2.2 para gerenciar o Kaspersky Security Service:

- **Controle total**: capacidade de visualizar e editar configurações gerais e permissões de usuário para o Kaspersky Security Service e iniciar e interromper o Kaspersky Security Service.
- **Ler**: capacidade de visualizar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
- **Modificação**: capacidade de visualizar e editar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
- **Execução**: capacidade de iniciar e interromper o Kaspersky Security Service.

É possível configurar também permissões de acesso avançadas: permitir ou negar acesso a funções específicas do Kaspersky Embedded Systems Security 2.2 (consulte a tabela abaixo).

Se você tiver configurado manualmente as permissões de acesso para um usuário ou grupo, o nível de acesso **Permissões especiais** será definido para este usuário ou grupo.

Tabela 18. Delimitação de permissões de acesso às funções do Kaspersky Embedded Systems Security 2.2

Recurso	Descrição
Visualização de configurações de serviço	Visualização: capacidade de visualizar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
Solicitação do status de serviço do Gerenciador de Serviço	Capacidade de solicitar o status de execução do Kaspersky Security Service a partir do Gerenciador de Controle de Serviço do Microsoft Windows.
Solicitação de status de serviço	Capacidade de solicitar o status de execução do Kaspersky Security Service.
Listar serviços dependentes	Capacidade de visualizar uma lista de serviços dos quais o Kaspersky Security Service depende e que dependem do Kaspersky Security Service.
Editar configurações de serviço	Capacidade de visualizar e editar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
Iniciar o serviço	Capacidade de iniciar o Kaspersky Security Service.
Parar o serviço	Capacidade de parar o Kaspersky Security Service.
Pausar/Reiniciar o serviço	Capacidade de pausar e reiniciar o Kaspersky Security Service.
Permissões de leitura	Capacidade de visualizar a lista de usuários do Kaspersky Security Service e os privilégios de acesso de cada usuário.
Permissões de edição	Capacidade para: • Adicionar e remover usuários do Kaspersky Security Service. • Editar permissões de acesso de usuário ao Kaspersky Security Service.
Excluir o serviço	Capacidade de anular o registro do Kaspersky Security Service no Gerenciador de Controle de Serviço do Microsoft Windows.
Solicitações ao serviço definidas pelo usuário	Capacidade de criar e enviar solicitações de usuário ao Kaspersky Security Service.

Registrar o Kaspersky Security Service como um serviço protegido

A tecnologia Protected Process Light (também conhecida como "PPL") assegura que o sistema operacional só carregue serviços e processos confiáveis. Para um serviço ser executado como serviço protegido, um driver *Early Launch Antimalware* deve ser instalado no computador protegido.

Um driver *Early Launch Antimalware* (também referido como "ELAM") fornece a proteção para os computadores na sua rede quando eles iniciam e antes que drivers de terceiros sejam inicializados.

O driver ELAM é instalado automaticamente durante a instalação do Kaspersky Embedded Systems Security 2.2 e usado para registrar o Kaspersky Security Service como um PPL quando o sistema operacional é inicializado. Quando o Kaspersky Security Service (kavfs.exe) é iniciado como um processo protegido do sistema, outros processos não protegidos no sistema não são capazes de injetar threads, gravar na memória virtual do processo protegido ou parar o serviço.

Quando um processo é iniciado como um PPL, ele não pode ser gerenciado pelo usuário desconsiderando as permissões de usuário configuradas. O registro do Kaspersky Security Service como PPL usando o driver ELAM é compatível com o Microsoft Windows 10 e sistemas operacionais posteriores. Se você instalar o Kaspersky Embedded Systems Security 2.2 em um computador executando um sistema operacional compatível com PPL, o gerenciamento de permissões para o Kaspersky Security Service (KAVFS) não estará disponível.

O Kaspersky Security Service inicia todos os processos filhos como PPLs.

► *Para instalar o Kaspersky Embedded Systems Security 2.2 como PPL, execute o seguinte comando:*

```
msiexec /i ks4ws_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Você pode usar a linha de comando para configurar o uso do PPL.

Sobre permissões de acesso para o Kaspersky Security Management Service

Você pode revisar a lista de serviços do Kaspersky Embedded Systems Security 2.2.

Durante a instalação, o Kaspersky Embedded Systems Security 2.2 registra o Kaspersky Security Management Service (KAVFSGT). Para gerenciar o aplicativo por meio do Console do Aplicativo instalado em um computador diferente, a conta cujas permissões são usadas para conectar ao Kaspersky Embedded Systems Security 2.2 deve ter acesso total ao Kaspersky Security Management Service no computador protegido.

Por padrão, o acesso ao Kaspersky Security Management Service é concedido aos usuários do grupo Administradores no computador protegido e aos usuários do grupo Administradores do ESS criado no computador protegido durante a instalação do Kaspersky Embedded Systems Security 2.2.

É possível gerenciar o Kaspersky Security Management Service apenas por meio do snap-in **Serviços** do Microsoft Windows.

Você não pode permitir ou bloquear o acesso ao Kaspersky Security Management Service configurando o Kaspersky Embedded Systems Security 2.2.

Você pode conectar ao Kaspersky Embedded Systems Security 2.2 a partir de uma conta local se existir uma conta com o mesmo nome e senha registrada no computador protegido.

Configurar permissões de acesso para o Kaspersky Embedded Systems Security 2.2 e o Kaspersky Security Service

Você pode editar a lista de usuários e os grupos de usuário com permissão para acessar as funções do Kaspersky Embedded Systems Security 2.2 e gerenciar o Kaspersky Security Service, e também editar as permissões de acesso desses usuários e grupos de usuário.

► *Para adicionar ou remover um usuário ou grupo da lista:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política ativa do Kaspersky Security Center e essa política bloquear alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Suplementar**, execute uma das seguintes etapas:
   - Selecione **Permissões de acesso do usuário para gerenciamento do aplicativo** se desejar editar a lista de usuários com permissões de acesso para funções do Kaspersky Embedded Systems 2.2.
   - Selecione **Permissões de acesso do usuário para gerenciamento do Security Service** se desejar editar a lista de usuários com permissões de acesso para gerenciar o Kaspersky Security Service.

   A janela **Permissões do grupo do Kaspersky Embedded Systems Security 2.2** é exibida.
4. Na janela exibida, execute as seguintes operações:
   - Para adicionar um usuário ou grupo à lista, clique no botão **Adicionar** e selecione o usuário ou grupo a quem deseja conceder privilégios.
   - Para remover um usuário ou grupo da lista, selecione o usuário ou grupo cujo acesso deseja restringir e clique no botão **Remover**.
5. Clique no botão **Aplicar**.

Os usuários selecionados (grupos) são adicionados ou removidos.

► *Para editar permissões de um usuário ou grupo para gerenciar o Kaspersky Embedded Systems Security 2.2 ou o Kaspersky Security Service:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Suplementar**, execute uma das seguintes etapas:
   - Selecione **Modificar direitos de gerenciamento de aplicativos do usuário** se desejar editar a lista de usuários que têm permissões de acesso às funções de gerenciamento do Kaspersky Embedded Systems Security 2.2.
   - Selecione **Modificar direitos do usuário do Kaspersky Security Management Service** se desejar editar a lista de usuários que têm permissões de acesso para gerenciar o aplicativo por meio do Kaspersky Security Service.

   A janela de grupo **Permissões para o Kaspersky Embedded Systems Security** é exibida.
4. Na janela exibida, na lista **Grupos ou usuários**, selecione o usuário ou grupo de usuários para os quais deseja alterar as permissões.
5. Na seção **Permissões para o grupo "<Usuário (Grupo)>"**, selecione as caixas de seleção **Permitir** ou **Bloquear** para os seguintes níveis de acesso:
   - **Controle total**: conjunto completo de permissões para gerenciar o Kaspersky Embedded Systems Security 2.2 ou o Kaspersky Security Service.
   - **Ler**:
     - As seguintes permissões para gerenciar o Kaspersky Embedded Systems Security 2.2: **Recuperar estatísticas**, **Ler configurações**, **Ler logs** e **Permissões de leitura**.
     - As seguintes permissões para gerenciar o Kaspersky Security Service: **Ler as configurações de serviço**, **Solicitar status de serviço do Service Control Manager**, **Solicitar status do serviço**, **Ler lista de serviços dependentes**, **Permissões de leitura**.
   - **Modificação**:
     - Todas as permissões para gerenciar o Kaspersky Embedded Systems Security 2.2, exceto **Editar permissões**;
     - As seguintes permissões para gerenciar o Kaspersky Security Service: **Modificar configurações do serviço**, **Permissões de leitura**.
   - **Execução**: as seguintes permissões para gerenciar o Kaspersky Security Service: **Inicialização**

do serviço, **Interrupção do serviço**, **Pausar/retomar serviço**, **Permissões de leitura**, **Solicitações de serviço definidas pelo usuário**.

6. Para definir as configurações avançadas de permissões para um usuário ou grupo (**Permissões especiais**), clique no botão **Avançado**.
   a. Na janela **Configurações avançadas de segurança para o Kaspersky Embedded Systems Security 2.2** exibida, selecione o usuário ou grupo que deseja.
   b. Clique no botão **Editar**.
   c. Na lista suspensa na parte superior da janela, selecione o tipo do controle de acesso (**Permitir** ou **Bloquear**).
   d. Selecione as caixas de seleção opostas às funções que deseja permitir ou bloquear para o usuário ou grupo selecionado.
   e. Clique em **OK**.
   f. Na janela **Configurações de segurança avançadas para o Kaspersky Embedded Systems Security 2.2**, clique em **OK**.
7. Na janela do grupo **Permissões para o Kaspersky Embedded Systems Security**, clique no botão **Aplicar**.

As permissões configuradas para o gerenciamento do Kaspersky Embedded Systems Security 2.2 ou para o Kaspersky Security Service são salvas.

Acesso protegido por senha às funções do Kaspersky Embedded Systems Security 2.2

Você pode restringir o acesso ao gerenciamento do aplicativo e aos serviços registrados configurando permissões de usuário (consulte a seção "Permissões de acesso às funções do Kaspersky Embedded Systems Security 2.2" na página 77). Também é possível estabelecer uma proteção por senha nas configurações do Kaspersky Embedded Systems Security 2.2 para uma proteção adicional da execução de operações críticas.

O Kaspersky Embedded Systems Security 2.2 solicita uma senha quando você tenta acessar as seguintes funções de aplicativo:

- conexão ao Console do Aplicativo;
- desinstalação do Kaspersky Embedded Systems Security 2.2;
- modificação dos componentes do Kaspersky Embedded Systems Security 2.2.
- execução de comandos via linha de comando.

A interface do Kaspersky Embedded Systems Security 2.2 oculta a senha especificada na tela. O Kaspersky Embedded Systems Security 2.2 armazena a senha como uma soma de verificação calculada quando esta é especificada.

É possível exportar e importar uma configuração de aplicativo protegida por senha. O arquivo de configuração, criado como resultado de uma exportação da configuração de aplicativo protegida, contém a soma de verificação da senha e o valor do modificador utilizado para preencher a linha da senha.

Não modifique a soma de verificação ou o modificador no arquivo de configuração. Importar uma configuração protegida por senha que tenha sido alterada manualmente pode fazer com que o acesso ao aplicativo seja bloqueado inteiramente.

► *Para proteger o acesso às funções do Kaspersky Embedded Systems Security 2.2, siga estas etapas:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados**. Expanda o grupo de administração com os computadores cujas configurações de aplicativo você deseja configurar.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir configurações de política para um grupo de computadores, selecione a guia **Políticas** e abra as **Propriedades de <nome da política>>**.
   - Se você quiser definir as configurações do aplicativo para um único computador, abra as configurações necessárias nas **Configurações do aplicativo** (consulte a seção "**Definindo tarefas locais na janela de Configurações do aplicativo do Kaspersky Security Center**" na página 101) a janela no Kaspersky Security Center.
3. Na seção **Segurança**, clique no botão **Configurações**.

   A janela **Configurações de segurança** é exibida.
4. Na seção **Configurações de proteção de senha**, marque a caixa de seleção **Aplicar proteção de senha**.

   Os campos **Senha** e **Confirmar senha** ficam ativos.
5. No campo **Senha**, insira o valor que você deseja usar para proteger o acesso às funções do Kaspersky Embedded Systems Security 2.2.
6. No campo **Confirmar senha**, insira a sua senha novamente.
7. Clique em **OK**.

As configurações especificadas são salvas. O Kaspersky Embedded Systems Security 2.2 solicitará a senha especificada para acessar as funções protegidas.

Esta senha não pode ser recuperada. A perda da senha resulta na perda completa do controle do aplicativo. Além disso, será impossível desinstalar o aplicativo do computador protegido.

É possível alterar ou redefinir a senha especificada nas configurações do aplicativo a qualquer momento.

► *Para redefinir a senha,*

Desmarque a caixa de seleção **Aplicar proteção de senha** na política ou nas configurações do aplicativo.

A Proteção por senha será desativada. O Kaspersky Embedded Systems Security 2.2 exclui a soma de verificação da senha antiga das configurações do aplicativo.

Ativar conexões de rede para o Kaspersky Security Management Service

Os nomes de configurações podem variar em diferentes sistemas operacionais Windows.

► *Para permitir conexões de rede para o Kaspersky Security Management Service no computador protegido, siga estas etapas:*

1. Em um computador protegido executando o Microsoft Windows, selecione **Iniciar > Painel de controle > Segurança > Firewall do Windows**.
2. Na janela **Configurações do Firewall do Windows**, selecione **Alterar** configurações.
3. Na lista de exclusões predefinidas da guia **Exclusões**, marque as seguintes caixas de seleção: **Acesso COM + rede**, **Windows Management Instrumentation (WMI)** e **Administração Remota**.
4. Clique no botão **Adicionar programa**.
5. Selecione o arquivo kavfsgt.exe na janela **Adicionar programa**. Este arquivo é armazenado na pasta que você especificou como a pasta de destino durante a instalação do Console do Aplicativo.
6. Clique em **OK**.
7. Clique em **OK** na janela **Configurações do Firewall do Windows**.

As conexões da rede para o Kaspersky Security Management Service no computador protegido serão permitidas.

Criando e configurando políticas

Esta seção fornece informações sobre a utilização de políticas do Kaspersky Security Center para gerenciar o Kaspersky Embedded Systems Security 2.2 em vários computadores.

Neste capítulo

Sobre as políticas

As políticas globais do Kaspersky Security Center podem ser criadas para gerenciar a proteção em vários computadores em que o Kaspersky Embedded Systems Security 2.2 está instalado.

Uma política impõe as configurações, funções e tarefas do Kaspersky Embedded Systems Security 2.2 especificadas nela a todos os computadores protegidos de um grupo de administração.

Várias políticas podem ser criadas e impostas alternadamente para um grupo de administração. A política atualmente ativa para um grupo tem o status *ativo* no Console de Administração.

As informações sobre a imposição da política são registradas no log de auditoria do sistema do Kaspersky Embedded Systems Security 2.2. Essas informações podem ser visualizadas no Console do Aplicativo no nó **Log de auditoria do sistema**.

O Kaspersky Security Center oferece uma maneira para aplicar políticas em computadores locais: *Proibir a alteração das configurações*. Após uma política ter sido aplicada, o Kaspersky Embedded Systems Security 2.2 usa os valores de configurações junto dos quais você selecionou o ícone nas propriedades de política em computadores locais, ao invés dos valores para aquelas configurações que eram verdadeiras antes da política ser aplicada. O Kaspersky Embedded Systems Security 2.2 não aplica os valores de configurações de política ativa junto dos quais o ícone é selecionado nas propriedades de política.

Se uma política estiver ativa, os valores de configurações marcadas com o ícone na política são exibidos no Console do Aplicativo, mas não podem ser editados. Os valores de outras configurações (marcados com o ícone na política) podem ser editados no Console do Aplicativo.

As configurações definidas na política ativa e marcadas com o ícone também bloqueiam alterações no Kaspersky Security Center para um computador na janela **Propriedades: <Nome do computador>**.

As configurações especificadas e enviadas para o computador local usando uma política ativa são salvas nas configurações de tarefas locais após a política ativa ser desativada.

Se a política definir as configurações para qualquer tarefa de Proteção em Tempo Real e se essa tarefa estiver em execução atualmente, as configurações definidas pela política serão modificadas assim que a política for aplicada. Se a tarefa não estiver sendo executada, as configurações serão aplicadas quando ela for iniciada.

Criando políticas

O processo de criação de uma política envolve as seguintes etapas:

1. Criando uma política usando o assistente de políticas. As configurações de tarefas de Proteção do Computador em Tempo Real podem ser definidas usando as caixas de diálogo do assistente.
2. Definindo as configurações de política. Na janela **Propriedades: <Nome da política>** da política criada, você pode definir as configurações de tarefas de Proteção do Computador em Tempo Real, as configurações gerais do Kaspersky Embedded Systems Security 2.2, as configurações de Quarentena e Backup, o nível de detalhe dos logs de tarefas, bem como notificações de administrador e de usuário sobre eventos do Kaspersky Embedded Systems Security 2.2.

► *Para criar uma política para um grupo de computadores que executam o Kaspersky Embedded Systems Security 2.2, siga as seguintes etapas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e, em seguida, selecione o grupo de administração que contém os computadores para os quais deseja criar uma política.
2. No painel de detalhes do grupo de administração selecionado, selecione a guia **Políticas** e clique no link **Criar uma política** para iniciar o assistente e criar uma política.

   A janela **Assistente de Nova Política** é exibida.
3. Na janela **Selecione o aplicativo para o qual deseja criar uma política de grupo**, selecione Kaspersky Embedded Systems Security 2.2 e clique em **Avançar**.
4. **Insira um nome de política de grupo** no campo **Nome**.

   > O nome da política não pode conter os seguintes símbolos: `" * < : > ? \ | .`

5. Para aplicar a configuração de política usada para a versão anterior do aplicativo:
   a. Marque a caixa de seleção **Usar configurações da política de versões anteriores do aplicativo**.
   b. Clique no botão **Procurar** e selecione a política que deseja aplicar.
   c. Clique em **Avançar**.
6. Na janela **Seleção do tipo de operação**, selecione uma das seguintes opções:
   - **Novo**, para criar uma nova política com configurações padrão.
   - **Importar política criada com a versão anterior do Kaspersky Embedded Systems Security** para usar tal versão da política como modelo.
   - Clique em **Procurar** e selecione um arquivo de configuração no qual uma política existente está armazenada.
7. Na janela **Proteção do Computador em Tempo Real**, configure a Proteção de Arquivos em Tempo Real, as tarefas de Uso da KSN e a funcionalidade de Prevenção de Exploits conforme necessário. Permita ou bloqueie o uso de tarefas de política configuradas em computadores locais na rede:
   - Clique no botão para permitir alterações nas configurações de tarefa em computadores de rede e para bloquear a aplicação de configurações de tarefa definidas na política.
   - Clique no botão para negar alterações nas configurações de tarefa em computadores de rede e para permitir a aplicação de configurações de tarefa definidas na política.

A política recém-criada usa as configurações padrão das tarefas de Proteção do Computador em Tempo Real.

- Para editar as configurações padrão da tarefa de Proteção de Arquivos em Tempo Real, clique no botão **Configurações** na seção **Proteção de Arquivos em Tempo Real**. Na janela exibida, configure a tarefa de acordo com as suas necessidades. Clique em **OK**.
- Para editar as configurações padrão da tarefa de Uso da KSN, clique no botão **Configurações** na seção **Uso da KSN**. Na janela exibida, configure a tarefa de acordo com as suas necessidades. Clique em **OK**.

  Para iniciar a tarefa de Uso da KSN, é necessário aceitar a Declaração da KSN na janela Manuseio de dados (consulta a seção "Configurando o processamento de dados" na página 167).

- Para editar as configurações padrão do componente Prevenção de Exploits, clique no botão **Configurações** na seção **Prevenção de Exploits**. Na janela exibida, configure a funcionalidade de acordo com a sua necessidade. Clique em **OK**.

8. Selecione um dos seguintes status de política na janela **Criar política de grupo para o aplicativo**:
   - **Política ativa** se quiser aplicar a política imediatamente após sua criação. Se uma política ativa já existir no grupo, ela será desativada e uma nova política será aplicada.
   - **Política inativa**, se não quiser aplicar a política criada imediatamente. Nesse caso, a política poderá ser ativada mais tarde.
   - Selecione caixa de seleção **Abrir propriedades da política imediatamente após serem criadas** para fechar automaticamente o **Assistente de Nova Política** e configurar a política recém-criada após clicar no botão **Avançar**.
9. Clique no botão **Concluir** na janela do Assistente **Concluindo o Assistente**.

A política criada é exibida na lista de políticas, na guia **Políticas** do grupo de administração selecionado. Na janela **Propriedades: <Nome da política>**, você pode definir outras configurações, tarefas e funções do Kaspersky Embedded Systems Security 2.2.

Configurando políticas

Na janela **Propriedades de <Nome da política>** de uma política existente, você pode definir as configurações gerais do Kaspersky Embedded Systems Security 2.2, configurações de Quarentena e de Backup, configurações da Zona Confiável, configurações da Proteção em Tempo Real, configurações de Controle de Atividades Locais, o nível de detalhes para logs de tarefas, bem como notificações de usuários e de administrador sobre os eventos do Kaspersky Embedded Systems Security 2.2, privilégios de acesso para gerenciar o aplicativo e o Kaspersky Security Service e as configurações do aplicativo do perfil de política.

► *Para definir as configurações de política:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Expanda o grupo de administração para o qual deseja definir as configurações de política associadas e abra o nó filho **Políticas** no painel detalhes.

3. Selecione uma política que deseja configurar e abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - Selecionando a opção **Propriedades** no menu de contexto de política.
   - Clicando no link **Configurar política** no painel de detalhes à direita da política selecionada.
   - Clicando duas vezes na política selecionada.
4. Na guia **Geral** na seção **Status de política**, ative ou desative a política. Para fazer isso, selecione uma das opções a seguir:
   - **Política ativa**, se deseja que a política seja aplicada a todos os computadores dentro do grupo de administração selecionado.
   - **Política inativa**, se não deseja que a política seja aplicada a todos os computadores dentro do grupo selecionado.

   A configuração **Política de usuário ausente** não está disponível ao gerenciar o Kaspersky Embedded Systems Security 2.2.
5. Nas seções **Notificação de evento**, **Configurações de aplicativo**, **Logs e notificações**, **Suplementar**, **Histórico de revisão**, você pode modificar a configuração do aplicativo (consulte a tabela abaixo).
6. Nas seções **Proteção do Computador em Tempo Real**, **Controle de Atividades Locais**, **Controle de atividade de rede** e **Inspeção do Sistema**, defina as configurações do aplicativo e de sua inicialização (consulte a tabela abaixo).

   Você pode ativar ou desativar a execução de qualquer tarefa em todos os computadores dentro do grupo de administração por meio de uma política do Kaspersky Security Center.
   Você pode configurar a aplicação de configurações de política em todos os computadores de rede para cada componente de software individual.
7. Clique em **OK**.

As configurações definidas são aplicadas na política.

Instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo por meio do Console do Aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

Seções com configurações de política do Kaspersky Embedded Systems Security 2.2

Geral

Na seção **Geral**, é possível definir as seguintes configurações de política:

- Indicar o status da política.
- Configurar a herança de configurações das políticas pais e políticas filhas.

Notificações de evento

Na seção **Notificações de evento**, você pode definir configurações para as seguintes categorias de evento:

- *Eventos críticos*
- *Falha*
- *Aviso*
- *Evento informativo*

É possível usar o botão **Propriedades** para definir as seguintes configurações para os eventos selecionados:

- Indicar o local de armazenamento e o período de retenção das informações sobre os eventos registrados.
- Indicar o método de notificação sobre eventos registrados.

Configurações do aplicativo

Tabela 19. Configurações da seção Configurações do aplicativo

Seção	Opções
Escalabilidade e interface	Na seção **Escalabilidade e interface**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Optar pela definição manual ou automática das configurações de escalabilidade. • Definir as configurações de exibição de ícone de aplicativo.
Segurança	Na seção **Segurança e confiabilidade**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Definir as configurações de execução de tarefa. • Especificar como o aplicativo deve se comportar quando o computador estiver funcionando com a fonte de energia UPS. • Ativar ou desativar a proteção por senha das funções do aplicativo.
Conexões	Na seção **Conexões**, é possível usar o botão **Configurações** para definir os seguintes parâmetros de servidor proxy para se conectar a servidores de atualização, servidores de ativação e à KSN: • Definir as configurações do servidor proxy. • Especificar as configurações de autenticação do servidor proxy.
Executar tarefas do sistema	Na subseção **Executar tarefas do sistema**, é possível usar o botão **Configurações** para permitir ou bloquear a inicialização das seguintes tarefas do sistema de acordo com uma programação definida em computadores locais: • Tarefa de Verificação por Demanda. • Tarefas Atualização e Copiar atualizações.

Suplementar

Tabela 20. Configurações da seção Suplementar

Seção	Opções
Zona Confiável	Clique no botão **Configurações** na seção **Zona Confiável** para definir as seguintes configurações da Zona Confiável do aplicativo: • Criar uma lista de exclusões da Zona Confiável. • Ativar ou desativar a verificação de operações de backup de arquivos. • Criar uma lista de processos confiáveis.
Verificação de unidades removíveis	Clique no botão **Configurações** para definir as configurações da verificação de unidades USB removíveis.
Permissões de acesso do usuário para gerenciamento do aplicativo	Nesta seção, é possível configurar os direitos do usuário e do grupo de usuários para gerenciar o Kaspersky Embedded Systems Security 2.2.

Seção	Opções
Permissões de acesso do usuário para gerenciamento do Security Service	Nesta seção, é possível configurar os direitos do usuário e do grupo de usuários para gerenciar o Kaspersky Security Service.
Armazenamentos	Na subseção **Armazenamentos**, clique no botão **Configurações** para definir as seguintes configurações de Quarentena e Backup: • Especificar o caminho da pasta na qual deseja colocar objetos em Quarentena ou de Backup. • Configurar o tamanho máximo de Backup e Quarentena e também especificar o limite de espaço livre. • Especificar o caminho da pasta na qual deseja colocar os objetos restaurados de Quarentena ou de Backup. • Configurar a transmissão de informações sobre objetos de Quarentena e de Backup ao Servidor de Administração.

Proteção do Computador em Tempo Real

Tabela 21. Configurações da seção Proteção do Computador em Tempo Real

Seção	Opções
Proteção de Arquivos em Tempo Real	Na seção **Proteção de Arquivos em Tempo Real**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Indicar o modo de proteção. • Configurar o uso do Analisador Heurístico. • Configurar o uso da Zona Confiável. • Indicar o escopo da proteção. • Definir o nível de segurança para o escopo da proteção selecionado: você pode selecionar um nível de segurança predefinido ou definir manualmente as configurações de segurança. • Definir as configurações de inicialização da tarefa.
Uso da KSN	Na subseção **Uso da KSN**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Indicar as ações a serem executadas em objetos não confiáveis da KSN. • Configurar a transferência de dados e o uso do Kaspersky Security Center como um servidor proxy da KSN. Clique no botão **Manuseio de dados** para aceitar ou rejeitar a Declaração da KSN e definir configurações de troca de dados seguras.
Prevenção de Exploits	Na seção **Prevenção de Exploits**, é possível clicar no botão **Configurações** para definir as seguintes configurações da tarefa: • Selecionar o modo de proteção da memória do processo. • Indicar as ações para reduzir os riscos de exploit. • Adicionar e editar a lista de processos protegidos.

Controle de Atividades Locais

Tabela 22. Configurações da seção Controle de Atividades Locais

Seção	Opções
Controle de Inicialização de Aplicativos	Na seção **Controle de Inicialização de Aplicativos**, é possível usar o botão **Configurações** para definir as seguintes configurações de tarefa: • Selecionar o modo de operação da tarefa. • Definir configurações para controlar as inicializações subsequentes de aplicativo. • Indicar o escopo para o aplicativo das regras do Controle de Inicialização de Aplicativos. • Configurar o uso da KSN. • Definir as configurações de inicialização da tarefa.
Controle de Dispositivos	Na seção **Controle de Dispositivos**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Selecionar o modo de operação da tarefa. • Definir as configurações de inicialização da tarefa.

Controle de atividade de rede

Tabela 23. Configurações da seção Controle de atividade de rede

Seção	Opções
Gerenciamento de Firewall	Na seção **Gerenciamento de Firewall**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Configurar as regras de Firewall. • Definir as configurações de inicialização da tarefa.

Inspeção do sistema

Tabela 24. Configurações da seção Inspeção do Sistema

Seção	Opções
Monitor de Integridade de Arquivos	Na seção **Monitor de Integridade de Arquivos**, é possível configurar o controle sobre as modificações em arquivos que podem significar uma violação de segurança em um computador protegido.
Inspeção do Log	Na seção **Inspeção do Log**, é possível configurar um controle de integridade do computador protegido com base nos resultados da análise de Log de Eventos do Windows.

Logs e Notificações

Tabela 25. Configurações da seção Logs e Notificações

Seção	Opções
Logs de tarefas	Na seção **Log de tarefas**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Especificar o nível de importância dos eventos registrados para os componentes de software selecionados. • Especificar as configurações de armazenamento de logs de tarefas. • Especificar a integração SIEM com configurações do Kaspersky Security Center.
Notificações de evento	Na seção **Notificações de evento**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Especificar as configurações de notificação de usuário para o evento *Objeto detectado*. • Especificar as configurações de notificação de administrador para qualquer evento selecionado na lista de eventos na seção **Configurações de notificação**.
Interação com o Servidor de Administração	Na seção **Interação com o Servidor de Administração**, é possível clicar no botão **Configurações** para selecionar os tipos de objetos que o Kaspersky Embedded Systems Security 2.2 relatará ao Servidor de Administração.

Histórico de revisão

Na seção **Histórico de revisão**, é possível gerenciar revisões: comparar com a revisão atual ou outra política, adicionar descrições de revisões, salvar revisões em um arquivo ou realizar uma reversão.

Configurando a inicialização programada de tarefas locais de sistema

É possível usar políticas para permitir ou bloquear a inicialização da tarefa de Verificação por Demanda e da tarefa de Atualização do sistema local de acordo com a programação configurada localmente em cada computador no grupo de administração:

- Se a inicialização programada de um tipo específico de tarefa local do sistema for proibida por uma política, essas tarefas não serão realizadas no computador local de acordo com a programação. É possível iniciar tarefas locais do sistema manualmente.
- Se a inicialização programada de um tipo específico de tarefa local do sistema for permitida por uma política, essas tarefas serão realizadas de acordo com os parâmetros programados configurados localmente para essa tarefa.

Por padrão, a inicialização de tarefas locais do sistema é proibida pela política.

> Recomendamos que você não permita que tarefas locais do sistema sejam iniciadas sem atualizações ou verificações por demanda estiverem sendo administradas por tarefas de grupo do Kaspersky Security Center.

Se você não usar tarefas de atualização de grupo ou de verificação por demanda, permita a inicialização das tarefas locais do sistema na política: o Kaspersky Embedded Systems Security 2.2 realizará atualizações do banco de dados e do módulo do aplicativo e iniciará todas as tarefas de verificação por demanda do sistema local de acordo com a programação padrão.

Você pode usar políticas para permitir ou bloquear a inicialização programada das tarefas locais de sistema a seguir:

- Tarefas de Verificação por Demanda: Verificação de Áreas Críticas, Verificação da Quarentena, Verificação na Inicialização do Sistema Operacional, Verificação de Integridade de Módulos de Software.
- Tarefas de Atualização: Atualização do Banco de Dados, Atualizações dos Módulos de Software e Copiar Atualizações.

Se o computador protegido for excluído do grupo de administração, a programação de tarefas do sistema será ativada automaticamente.

► *Para permitir ou bloquear a inicialização programada de tarefas do sistema do Kaspersky Embedded Systems Security 2.2 em uma política, siga as etapas a seguir:*

1. No nó **Dispositivos gerenciados** da árvore do Console de Administração, expanda o grupo requerido e selecione a guia **Políticas**.
2. Na guia **Políticas**, no menu de contexto da política para a qual você deseja configurar o início programado de tarefas do sistema do Kaspersky Embedded Systems Security 2.2 nos computadores do grupo, selecione o comando **Propriedades**.
3. Na janela **Propriedades: <Nome da política>**, abra a seção **Configurações do aplicativo**. Na seção **Executar tarefas do sistema**, clique no botão **Configurações** e faça o seguinte:
   - Marque as caixas de seleção **Permitir a inicialização de tarefas de verificação por demanda** e **Permitir a inicialização de tarefas de atualização e de tarefas de Copiar atualizações** para permitir a inicialização programada das tarefas listadas.
   - Desmarque as caixas **Permitir inicialização de tarefas de verificação por demanda** e **Permitir a inicialização de tarefas de atualização e de tarefas de Copiar atualizações** para desativar a inicialização programada das tarefas listadas.

   Marcar ou desmarcar a caixa de seleção não irá afetar as configurações de inicialização de quaisquer tarefas locais personalizadas desse tipo.
4. Assegurar-se de que a política (consulte a seção "Sobre políticas" na página 88) que está configurando esteja ativa e tenha sido aplicada ao grupo selecionado de computadores.
5. Clique em **OK**.

As configurações de inicialização da tarefa programada são aplicadas às tarefas selecionadas.

Criando e configurando uma tarefa usando o Kaspersky Security Center

Esta seção contém informação sobre tarefas do Kaspersky Embedded Systems Security 2.2 e como criá-las, definir suas configurações, iniciá-las e interrompê-las.

Neste capítulo

Sobre a criação de tarefa no Kaspersky Security Center

Você pode criar tarefas de grupo para grupos de administração e conjuntos de computadores. Você pode criar os seguintes tipos de tarefa:

- Ativação do aplicativo
- Copiar atualizações
- Atualização do Banco de Dados
- Atualização dos Módulos de Software
- Reversão da Atualização do Banco de Dados
- Verificação por Demanda
- Controle de Integridade de Aplicativos
- Gerador de Regras de Controle de Inicialização de Aplicativos
- Gerador de Regras de Controle de Dispositivos

Você pode criar tarefas de grupo e locais das seguintes maneiras:

- para um computador: na janela **Propriedades <Nome de computador>** na seção **Tarefas**.
- para um grupo de administração: no painel de detalhes do nó do grupo selecionado de computadores na guia **Tarefas**.
- para um conjunto de computadores: no painel de detalhes do nó **Seleções de dispositivo**.

Usando políticas é possível desativar programações para tarefas de atualização e Verificação por Demanda de sistema locais (consulte a seção "Configurando a inicialização programada de tarefas locais de sistema" na página 95) em todos os computadores protegidos do mesmo grupo de administração.

Informações gerais sobre tarefas no Kaspersky Security Center são fornecidas na *Ajuda do Kaspersky Security Center.*

Criação de uma tarefa usando o Kaspersky Security Center

O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

► *Para criar uma nova tarefa no Console de Administração do Kaspersky Security Center:*

1. Inicie o assistente de tarefa de uma das seguintes maneiras:
   - Para criar uma tarefa local:
     a. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração e selecione o grupo ao qual o computador protegido pertence.
     b. No painel de detalhes, na guia **Dispositivos**, abra o menu de contexto do computador protegido e selecione **Propriedades**.
     c. Na janela exibida, clique no botão **Adicionar** na seção **Tarefas**.
   - Para criar uma tarefa de grupo:
     a. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo para o qual você deseja criar uma tarefa.
     b. No painel de detalhes, abra a guia **Tarefas** e selecione **Criar uma tarefa**.
   - Para criar uma tarefa para um conjunto personalizado de computadores, no nó **Seleções de dispositivo** na árvore do Console de Administração do Kaspersky Security Center, selecione **Criar uma tarefa**.

   A janela do assistente de tarefa é exibida.
2. Na janela **Selecionar o tipo de tarefa**, sob o título **Kaspersky Embedded Systems Security 2.2**, selecione o tipo da tarefa a ser criada.
3. Se você tiver selecionado qualquer tipo de tarefa, exceto Reversão da Atualização do Banco de Dados ou Ativação do Aplicativo, a janela **Configurações** é exibida. Dependendo do tipo de tarefa criada, execute uma das seguintes ações:
   - *Para criar uma tarefa de Verificação por Demanda*:
     a. Crie o escopo da verificação na janela **Escopo da verificação**.

        Por padrão, o escopo da verificação inclui áreas críticas do computador. Os escopos da verificação são marcados na tabela com o ícone ☑.

        Você pode alterar o escopo da verificação: adicione escopos, discos, pastas, objetos de rede e arquivos e atribua configurações de segurança específicas para cada escopo adicionado.

        - Para excluir todas as áreas críticas da verificação, abra o menu de contexto de cada linha e selecione a opção **Remover escopo**.
        - Para incluir um escopo de verificação, disco, pasta, objeto de rede ou arquivo predefinido no escopo da verificação, clique com o botão direito na tabela **Escopo da verificação** e selecione Adicionar escopo. Na janela **Adicionar objetos ao escopo da verificação**, selecione o escopo predefinido na lista **Escopo predefinido**, especifique a unidade

    do computador, pasta, objeto de rede ou arquivo no computador ou em outro computador da rede e clique no botão **OK**.

    - Para excluir subpastas ou arquivos da verificação, selecione a pasta adicionada (disco) na janela **Escopo da verificação** do assistente, abra o menu de contexto e selecione a opção **Configurar** e, em seguida, clique no botão **Configurações**, na janela Nível de segurança e, na janela **Configurações da Verificação por Demanda** da guia **Geral**, desmarque as caixas de seleção **Subpastas** e **Subarquivos**.
    - Para alterar as configurações de segurança do escopo da verificação, abra o menu de contexto do escopo cujas configurações você deseja definir e selecione **Configurar**. Na janela **Configurações da verificação por demanda**, selecione um dos níveis de segurança predefinidos ou clique no botão **Configurações** para definir as configurações de segurança manualmente. A definição das configurações de segurança é executada da mesma maneira que no Console do Kaspersky Embedded Systems Security 2.2.
    - Para ignorar objetos incorporados no escopo da verificação adicionado, abra o menu de contexto na tabela **Escopo da verificação**, selecione **Adicionar exclusão** e especifique os objetos que você deseja excluir: selecione um escopo predefinido na lista Escopo predefinido, especifique o disco do computador, pasta, objeto de rede ou arquivo em um computador protegido ou em outro computador da rede e clique no botão **OK**.
    - Os escopos da verificação excluídos são marcados com o ícone ☐ na tabela.

  b. Execute as ações seguintes na janela **Opções**.

     Selecione a caixa **Aplicar Zona Confiável** se deseja excluir os objetos descritos na Zona Confiável do Kaspersky Embedded Systems Security 2.2 do escopo da verificação da tarefa.

     Se você planeja usar a tarefa criada como uma tarefa de Verificação de Áreas Críticas, selecione a caixa **Executar tarefa em segundo plano** na janela **Opções**. O Kaspersky Security Center avalia a classificação de segurança do computador (computadores) em função dos resultados de desempenho de tarefas com o status de *Verificação de Áreas Críticas* e não somente pelos resultados de desempenho da tarefa do sistema **Verificação de Áreas Críticas**. Ao criar uma tarefa de Verificação por Demanda local, essa caixa de seleção não está disponível.

     Para atribuir a prioridade básica **Baixo** ao processo de trabalho onde a tarefa será executada, selecione a caixa de seleção **Executar tarefa em segundo plano** na janela **Opções**. Por padrão, os processos de trabalho em que as tarefas do Kaspersky Embedded Systems Security 2.2 são executadas têm a prioridade **Médio** (Normal). Ao reduzir a prioridade do processo, aumenta o tempo necessário para executar a tarefa, mas isso pode ter um efeito positivo sobre a velocidade de execução dos processos de outros programas ativos.

- *Para criar uma tarefa de atualização*, defina as configurações da tarefa de acordo com seus requisitos:

  a. Selecione a fonte de atualizações na janela **Fonte de atualização**.

  b. Clique no botão **Configurações de conexão**. A janela **Configurações de conexão** é aberta.

  c. Na janela **Configurações de conexão**:

     Especifique o modo do servidor FTP para conectar ao computador protegido.

     Modifique o tempo limite de conexão ao conectar à fonte de atualização, se necessário.

     Especifique as configurações de acesso do servidor proxy ao conectar com a fonte de atualização.

     Especifique a localização dos computadores protegidos, para otimizar o download de atualizações.

- *Para criar uma tarefa de Atualizações dos Módulos de Software*, defina as configurações de atualização dos módulos de programa necessárias na janela **Configurações para atualizações**

dos módulos de software do aplicativo:

a. Selecione Copiar e instalar atualizações críticas dos módulos de software ou apenas verificar a sua disponibilidade sem instalação.

b. Se **Copiar e instalar atualizações críticas dos módulos de software** estiver selecionado, um reinício do computador poderá ser necessário para aplicar os módulos de software instalados. Se você desejar que o Kaspersky Embedded Systems Security 2.2 reinicie o computador automaticamente após a conclusão da tarefa, selecione a caixa **Permitir reinício do sistema operacional**. Para desativar o reinício automático do computador após a conclusão da tarefa, desmarque a caixa de seleção **Permitir reinício do sistema operacional**.

c. Para obter informações sobre atualizações do módulo do Kaspersky Embedded Systems Security 2.2, selecione **Receber informações sobre as atualizações disponíveis programadas dos módulos de software**.

   A Kaspersky Lab não publica pacotes de atualizações planejados nos servidores de atualização para instalação automática; eles podem ser baixados manualmente no site da Kaspersky Lab. Pode ser configurada uma notificação do administrador sobre o evento **Nova atualização programada dos módulos de software disponível**. Isto conterá o URL do nosso site do qual as atualizações programadas podem ser baixadas.

- *Para criar a tarefa Copiar atualizações*, especifique o conjunto de atualizações e a pasta de destino na janela **Configurações de Copiar atualizações**.
- *Para criar a tarefa de Ativação do aplicativo*, na seção **Configurações de ativação** aplique o arquivo de chave que deseja usar para ativar o aplicativo. Marque a caixa **Usar como chave adicional** se desejar criar uma tarefa para renovar a licença.
- *Para criar a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos ou de Gerador de Regras de Controle de Dispositivos*, na janela **Configurações** especifique as configurações baseadas nas quais a lista de regras de permissão será criada:

  a. Especifique um prefixo para os nomes da regra (somente para a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos).

  b. Configure o escopo de uso das regras de permissão (somente para a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos). Clique no botão **Avançar**.

  c. Especifique as ações que a tarefa de permissão executará gerando regras de permissão (somente para a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos) e após a conclusão da tarefa.

4. Configure a programação da tarefa (você pode configurar uma programação para todos os tipos de tarefa, exceto a tarefa de Reversão da Atualização do Banco de Dados). Execute as ações seguintes na janela **Programação**:

   a. Selecione a caixa de seleção **Executar de acordo com o agendamento** para ativar a programação;

   b. Especifique a frequência de inicialização de tarefa: selecione um dos seguintes valores da lista **Frequência**: **De hora em hora**, **Diariamente**, **Semanalmente**, **Ao iniciar o aplicativo**, **Após a atualização do banco de dados do aplicativo** (a frequência de inicialização **Após o Servidor de Administração ter recuperado as atualizações** também pode ser especificada nas seguintes tarefas de grupo: Atualização do Banco de Dados e Atualizações dos módulos de software):

   - Se **De hora em hora** estiver selecionado, especifique o número de horas em **A cada <número> hora(s)** no grupo de configuração **Configurações de início da tarefa**.
   - Se **Diariamente** estiver selecionado, especifique o número de dias em **A cada <número> dia(s)** no grupo de configuração **Configurações de início da tarefa**.

- Se **Semanalmente** for selecionado, especifique o número de semanas em **A cada <número> semana(s)** no grupo de configuração **Configurações de início da tarefa**. Especifique os dias da semana nos quais a tarefa será iniciada (por padrão, às segundas-feiras).

c. No campo **Hora inicial**, especifique a hora em que a tarefa será iniciada; no campo **Data inicial**, especifique a data em que a programação ficará ativa.

d. Especifique as configurações de programação restantes se necessário: clique no botão **Avançado** e faça o seguinte na janela **Configurações de programação avançadas**:

- Especifique a duração máxima da execução da tarefa: insira o número de horas e minutos no campo **Duração**, no grupo de configuração **Configurações de interrupção de tarefa**.
- Especifique o intervalo de tempo em um período de 24 horas no qual a execução de uma tarefa é pausada, no grupo de configuração **Configurações de interrupção de tarefa** insira os valores de início e fim do intervalo nos campos **Pausar de** e **até**.
- Especifique a data em que a programação será desativada: selecione a caixa de seleção **Cancelar agendamento a partir de** e selecione a data em que o agendamento será desativado usando a janela **Calendário**.
- Ative o início de tarefas perdidas: selecione a caixa de seleção **Executar tarefas ignoradas**.
- Ative a configuração de distribuição da hora de início: selecione a caixa **Randomizar a hora de início da tarefa no intervalo de** e especifique o valor em minutos.

e. Clique em **OK**.

5. Se a tarefa criada for para conjuntos de computadores, selecione a rede (grupo) de computadores na qual a tarefa será executada.
6. Na janela **Especificando uma conta para a execução da tarefa**, especifique a conta na qual você deseja executar a tarefa.
7. Na janela **Definir nome da tarefa**, insira um nome para a tarefa (com menos de 100 caracteres) sem incluir os símbolos **" * < > ? \ | :** . É recomendado adicionar o tipo de tarefa ao seu nome (por exemplo, "Verificação por demanda de pastas compartilhadas").
8. Na janela **Conclusão da criação da tarefa**, selecione a caixa **Executar tarefa quando o assistente for concluído** se quiser que a tarefa seja iniciada logo após ser criada. Clique no botão **Concluir**.

A tarefa criada é exibida na lista de **Tarefas**.

Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center

► *Para definir configurações de tarefas locais ou gerais do aplicativo na janela Configurações do aplicativo para um único computador da rede, realize as seguintes tarefas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Servidor de Administração do Kaspersky Security Center e selecione o grupo ao qual o computador protegido pertence.
2. No painel de detalhes, selecione a guia **Dispositivos**.

3. Abra a janela **Propriedades: <Nome do computador>** de uma das seguintes maneiras:
   - Clique duas vezes no nome do computador protegido.
   - Abra o menu de contexto do nome do computador protegido e selecione o item **Propriedades.**

   A janela **Propriedades: <Nome do computador>** é exibida.
4. Para especificar as configurações da tarefa local, siga as etapas a seguir:
   a. Vá até a seção **Tarefas**.
      - Na lista de tarefas, selecione uma tarefa local para configurar.
      - Clique duas vezes no nome da tarefa na lista de tarefas.
      - Selecione o nome da tarefa e clique no botão **Propriedades**.
      - Escolha **Propriedades** no menu de contexto da tarefa selecionada.
5. Para definir as configurações do aplicativo, siga as etapas a seguir:
   a. Vá até a seção **Aplicativos**.
      - Na lista de aplicativos instalados, selecione um aplicativo para configurar.
      - Clique duas vezes no nome do aplicativo na lista de aplicativos instalados.
      - Selecione o nome do aplicativo na lista de aplicativos instalados e clique no botão **Propriedades.**
      - Abra o menu de contexto do nome do aplicativo na lista de aplicativos instalados e selecione o item **Propriedades**.

      Se um aplicativo estiver sob a política do Kaspersky Security Center e essa política proibir a alteração das configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

Configurando tarefas de grupo no Kaspersky Security Center

O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

► *Para configurar a tarefa de grupo para múltiplos computadores:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e seleciona o grupo de administração para o qual deseja configurar as tarefas de aplicativo.
2. No painel de detalhes de um grupo de administração selecionado, abra a guia **Tarefas**.
3. Na lista de tarefas de grupo criadas anteriormente, selecione uma tarefa que deseja configurar. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa na lista de tarefas criadas.
   - Selecione o nome da tarefa na lista de tarefas criadas e clique no link **Configurar tarefa**.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
4. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.

   Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

5. Dependendo do tipo de tarefa configurada, execute uma das seguintes ações:
   - Para configurar uma tarefa de Verificação por Demanda:
     a. Na seção **Escopo da verificação**, configure um escopo de verificação.
     b. Na seção **Opções**, configure o nível de prioridade e integração de tarefa com outros componentes de software.
   - Para configurar uma tarefa de atualização, ajuste as configurações da tarefa de acordo com suas necessidades:
     a. Na seção **Configurações**, defina as configurações de fonte de atualização e otimização de uso de subsistema de disco.
     b. Clique no botão **Configurações de conexão** para definir as configurações de conexão da fonte de atualização.
   - Para configurar a tarefa de Atualizações de Módulos de Software, na seção **Configurações para atualizações dos módulos de software do aplicativo** selecione uma ação a ser executada: copiar e instalar atualizações críticas de módulos de software ou somente verificá-las.
   - Para configurar a tarefa Copiar atualizações, especifique o conjunto de atualizações e a pasta de destino na seção **Configurações de Copiar atualizações**.

- Para configurar a tarefa de Ativação do aplicativo, na seção **Configurações de ativação**, aplique o arquivo de chave que deseja usar para ativar o aplicativo. Selecione a caixa **Usar como código de ativação ou chave adicional** se deseja adicionar um código de ativação ou chave para renovar a licença.
- Para configurar a geração automática de regras de permissão para o controle do computador, na seção **Configurações** especifique as configurações com base nas quais a lista de regras de permissão será criada.

6. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
7. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa. Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.
8. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**. Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.
9. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

As configurações de tarefas de grupo definidas recentemente são salvas.

As configurações de tarefas de grupo que estão disponíveis para configuração estão resumidas na tabela abaixo.

Tabela 26. Configurações de tarefas de grupo do Kaspersky Embedded Systems Security 2.2

Tipos de tarefas do Kaspersky Embedded Systems Security 2.2	Seção na janela Propriedades: <Nome da tarefa>	Configurações de tarefa
A geração automática de regras (consulte a seção "Tarefas de Gerador de Regras de Controle de Inicialização de Aplicativos e Gerador de Regras de Controle de Dispositivos" na página 108)	**Configurações**	Ao configurar a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos, você pode: • Alterar o escopo da proteção adicionando ou removendo os caminhos a pastas e especificando tipos de arquivo para os quais a inicialização é permitida por regras geradas automaticamente. • Considerar aplicativos atualmente em execução.
	Opções	Você pode especificar ações para execução enquanto cria regras de permissão para o controle de inicialização de aplicativos: • **Usar certificado digital** • **Usar o assunto e a miniatura de certificado digital** • **Se o certificado estiver ausente, use** • **Usar hash SHA256** • **Gerar regras para usuário ou grupo de usuários** Você pode definir as configurações para arquivos de configuração com listas de regras de permissão que o Kaspersky Embedded Systems Security 2.2 cria após a conclusão da tarefa.

Tipos de tarefas do Kaspersky Embedded Systems Security 2.2	Seção na janela Propriedades: <Nome da tarefa>	Configurações de tarefa
	Programação	Você pode definir as configurações da inicialização programada da tarefa.
A Ativação do Aplicativo (consulte a seção "Ativação da tarefa de Aplicativo" na página 110)	**Configurações de Ativação**	Para ativar o aplicativo ou renovar a data de expiração você pode adicionar uma chave.
	Programação	Você pode definir as configurações da inicialização programada da tarefa.
Copiar atualizações (consulte a seção "Tarefas de atualização" na página 111)	**Fonte de atualização**	Você pode especificar o Servidor de Administração do Kaspersky Security Center ou os servidores de atualização da Kaspersky Lab como fonte de atualização do aplicativo. Você também pode criar uma lista personalizada de fontes de atualização: adicionando servidores HTTP ou FTP personalizados ou pastas de rede manualmente e definindo-os como fontes de atualização. Você pode especificar o uso dos servidores de atualização da Kaspersky Lab, se os servidores personalizados manualmente não estiverem disponíveis.
	Janela **Configurações de conexão**	No grupo **Configurações de conexão da fonte de atualização** você pode especificar se a conexão a servidores de atualização da Kaspersky Lab ou a algum outro servidor deve ser estabelecida por meio do servidor proxy.
	Configurações de Copiar atualizações	Você pode especificar o conjunto de atualizações destinado à cópia. No campo **Pasta para armazenamento local de atualizações copiadas**, especifique um caminho para uma pasta que será usada pelo Kaspersky Embedded Systems Security 2.2 para armazenar atualizações copiadas.
	Programação	Você pode definir as configurações da inicialização programada da tarefa.

Tipos de tarefas do Kaspersky Embedded Systems Security 2.2	Seção na janela Propriedades: <Nome da tarefa>	Configurações de tarefa
Atualização do Banco de Dados (consulte a seção "Tarefas de atualização" na página 111)	**Configurações**	Você pode especificar o Servidor de Administração do Kaspersky Security Center ou servidores de atualização da Kaspersky Lab como a fonte de atualização do aplicativo no grupo **Fonte de atualização**. Você também pode criar uma lista personalizada de fontes de atualização: adicionando servidores HTTP ou FTP personalizados ou pastas de rede manualmente e definindo-os como fontes de atualização. Você pode especificar o uso dos servidores de atualização da Kaspersky Lab, se os servidores personalizados manualmente não estiverem disponíveis. Na seção Otimização de uso de E/S de disco, é possível configurar o recurso que reduz a carga de trabalho no subsistema de disco: • **Diminuir a carga na E/S de disco** • **RAM usada para otimização (MB)**
	Janela **Configurações de conexão**	No grupo **Configurações de conexão da fonte de atualização** você pode especificar se a conexão a servidores de atualização da Kaspersky Lab ou a algum outro servidor deve ser estabelecida por meio do servidor proxy.
	Programação	Você pode definir as configurações da inicialização programada da tarefa.
Atualização dos módulos de software (consulte a seção "Tarefas de atualização" na página 111)	**Fonte de atualização**	Você pode especificar o Servidor de Administração do Kaspersky Security Center ou os servidores de atualização da Kaspersky Lab como fonte de atualização do aplicativo. Você também pode criar uma lista personalizada de fontes de atualização: adicionando servidores HTTP ou FTP personalizados ou pastas de rede manualmente e definindo-os como fontes de atualização. Você pode especificar o uso dos servidores de atualização da Kaspersky Lab, se os servidores personalizados manualmente não estiverem disponíveis.
	Janela **Configurações de conexão**	No grupo **Configurações de conexão da fonte de atualização** você pode especificar se a conexão a servidores de atualização da Kaspersky Lab ou a algum outro servidor deve ser estabelecida por meio do servidor proxy.

Tipos de tarefas do Kaspersky Embedded Systems Security 2.2	Seção na janela Propriedades: <Nome da tarefa>	Configurações de tarefa
	Configurações para atualização dos módulos de software do aplicativo	Você pode especificar quais ações devem ser executadas pelo Kaspersky Embedded Systems Security 2.2 quando as atualizações críticas de módulo de software estão disponíveis ou já foram instaladas e também se o Kaspersky Embedded Systems Security 2.2 tiver que receber informações com relação às atualizações programadas.
	Programação	Você pode definir as configurações da inicialização programada da tarefa.
Verificação por demanda (consulte a seção "Criar uma tarefa de Verificação por Demanda" na página 113)	**Escopo da verificação**	É possível especificar um Escopo da verificação para a tarefa de Verificação por Demanda e definir configurações de nível de segurança.
	Janela **Configurações da verificação por demanda**	Você pode selecionar um dos níveis de segurança predefinidos ou personalizar o nível de segurança manualmente.
	Opções	É possível ativar ou desativar o uso do analisador heurístico da tarefa de Verificação por Demanda e estabelecer o nível de análise usando um controle deslizante no grupo **Analisador heurístico**. No grupo **Integração com outros componentes** você pode definir as seguintes configurações: • Aplicar Zona Confiável para tarefas de Verificação por Demanda. • Aplicar o Uso da KSN para tarefas de Verificação por Demanda. • Defina uma prioridade para a tarefa de Verificação por Demanda: executar a tarefa em segundo plano (prioridade baixa) ou considerar a tarefa como uma Verificação de áreas críticas.
	Programação	Você pode definir as configurações da inicialização programada da tarefa.
Verificação de Integridade de Módulos de Software (na página 112)	**Programação**	Você pode definir as configurações da inicialização programada da tarefa.

Para tarefas como Reversão da Atualização do Banco de Dados, você pode definir somente configurações de tarefa padrão nas seções **Notificação** e **Exclusões do escopo de tarefa**, controladas pelo Kaspersky Security Center. Para obter informações detalhadas sobre a definição das configurações destas seções, consulte a *Ajuda do Kaspersky Security Center*.

Nesta seção

Tarefas de Gerador de Regras de Controle de Inicialização de Aplicativos e Gerador de Regras de Controle de Dispositivos

► *Para configurar a tarefa de Gerador de Regras de Controle de Dispositivos ou Gerador de Regras de Controle de Inicialização de Aplicativos, faça o seguinte:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e seleciona o grupo de administração para o qual deseja configurar as tarefas de aplicativo.
2. No painel de detalhes de um grupo de administração selecionado, abra a guia **Tarefas**.
3. Na lista de tarefas de grupo criadas anteriormente, selecione uma tarefa que deseja configurar. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa na lista de tarefas criadas.
   - Selecione o nome da tarefa na lista de tarefas criadas e clique no link **Configurar tarefa**.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
4. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.
5. Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.
6. Na seção **Configurações**, é possível definir as seguintes configurações:
   - Alterar o escopo da proteção adicionando ou removendo os caminhos a pastas e especificando tipos de arquivo para os quais a inicialização é permitida por regras geradas automaticamente.
   - Considerar aplicativos atualmente em execução.
7. Na seção **Configurações**, é possível especificar ações para execução enquanto cria regras de permissão para o controle de inicialização de aplicativos:
   - **Usar certificado digital**

     Se esta opção estiver selecionada, a presença de um certificado digital será especificada como o critério de acionamento de regra nas configurações das regras de permissão geradas recentemente para o Controle de inicialização de aplicativos. O aplicativo permitirá agora a inicialização de programas iniciados usando arquivos com um certificado digital. Esta opção é recomendada se você quiser permitir a inicialização de qualquer aplicativo que seja confiável no sistema operacional.

     Esta opção é selecionada por padrão.
   - **Usar o assunto e a miniatura de certificado digital**

     A caixa ativa ou desativa o uso do assunto e da miniatura do certificado digital do arquivo como critério de acionamento de regras de permissão de Controle de inicialização de aplicativos. A seleção desta caixa permite a especificação de condições de verificação mais rigorosas para o certificado digital.

Se esta caixa estiver selecionada, os valores de assunto e da miniatura do certificado digital dos arquivos para os quais as regras serão geradas são estabelecidos como o critério de acionamento de regras de permissão de Controle de inicialização de aplicativos. O Kaspersky Embedded Systems Security 2.2 permitirá aplicativos que sejam iniciados usando arquivos com uma miniatura e um certificado digital especificado.

Ao selecionar esta caixa o acionamento de regras de permissão é fortemente restringido com base em um certificado digital, pois uma miniatura é um identificador único de um certificado digital e não pode ser forjada.

Se esta caixa estiver desmarcada, a existência de qualquer certificado digital confiável no sistema operacional é estabelecida como o critério de acionamento de regras de permissão de Controle de inicialização de aplicativos.

A caixa de seleção fica ativa se a opção **Usar certificado digital** estiver selecionada.

A caixa de seleção é selecionada por padrão.

- **Se o certificado estiver ausente, use**

  A lista suspensa que permite a seleção do critério de acionamento de regras de permissão de Controle de inicialização de aplicativos, se o arquivo usado para gerar a regra não tiver um certificado digital.

  - **Hash SHA256**. O valor da soma de verificação do arquivo, usado para gerar a regra, é estabelecido como o critério para acionamento de regras de permissão de Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com a soma de verificação especificada.
  - **Caminho do arquivo**. O caminho do arquivo, usado para gerar a regra, é estabelecido como o critério para acionamento de regras de permissão de Controle de inicialização de aplicativos. O aplicativo agora permitirá a inicialização de aplicativos iniciados usando arquivos localizados na guia especificada de pastas na tabela Criar regras de permissão para aplicativos das pastas.

- **Usar hash SHA256**

  Se esta opção estiver selecionada, o valor da soma de verificação do arquivo, usado para gerar a regra, será especificado como o critério de acionamento de regra nas configurações das regras de permissão geradas recentemente para o Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com o valor da soma de verificação especificado.

  Esta opção é recomendada para casos quando as regras geradas são necessárias para alcançar o nível de segurança mais alto: a soma de verificação do SHA256 pode ser aplicada como um ID único de arquivo. O uso da soma de verificação do SHA256 como critério para acionamento de regras restringe o escopo de uso da regra em até um arquivo.

- **Gerar regras para usuário ou grupo de usuários**.

  Campo que exibe um usuário e/ou grupo de usuários. O aplicativo controlará qualquer aplicativo executado pelo usuário e/ou grupo de usuários especificado.

  A seleção padrão é **Todos**.

Você pode definir as configurações para arquivos de configuração com listas de regras de permissão que o Kaspersky Embedded Systems Security 2.2 cria após a conclusão da tarefa.

8. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).

9. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa.
10. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

> Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

11. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

    As configurações de tarefas de grupo definidas recentemente são salvas.

Ativação da tarefa de Aplicativo

► *Para configurar uma Ativação da tarefa de Aplicativo, realize as seguintes etapas:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e seleciona o grupo de administração para o qual deseja configurar as tarefas de aplicativo.
2. No painel de detalhes de um grupo de administração selecionado, abra a guia **Tarefas**.
3. Na lista de tarefas de grupo criadas anteriormente, selecione uma tarefa que deseja configurar. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa na lista de tarefas criadas.
   - Selecione o nome da tarefa na lista de tarefas criadas e clique no link **Configurar tarefa**.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
4. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.
5. Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.
6. Na seção **Configurações de Ativação**, aplique o arquivo de chave que você deseja usar para ativar o aplicativo. Marque a caixa de seleção **Usar como chave adicional** se desejar adicionar uma chave para estender a licença.
7. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
8. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa.
9. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

> Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

10. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

    As configurações de tarefas de grupo definidas recentemente são salvas.

Tarefas de atualização

Para configurar as tarefas Copiar Atualizações, Atualização do Banco de Dados ou de Atualização dos Módulos de Software, faça o seguinte:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e seleciona o grupo de administração para o qual deseja configurar as tarefas de aplicativo.
2. No painel de detalhes de um grupo de administração selecionado, abra a guia **Tarefas**.
3. Na lista de tarefas de grupo criadas anteriormente, selecione uma tarefa que deseja configurar. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa na lista de tarefas criadas.
   - Selecione o nome da tarefa na lista de tarefas criadas e clique no link **Configurar tarefa**.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
4. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.

   > Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

5. Dependendo do tipo de tarefa configurada, execute uma das seguintes ações:
   - Na seção **Fonte de atualização**, defina as configurações de fonte de atualização e otimização de uso de subsistema de disco.
     a. Você pode especificar o Servidor de Administração do Kaspersky Security Center ou servidores de atualização da Kaspersky Lab como a fonte de atualização do aplicativo na seção **Fonte de atualização**. Você também pode criar uma lista personalizada de fontes de atualização: adicionando servidores HTTP ou FTP personalizados ou pastas de rede manualmente e definindo-os como fontes de atualização.

        Você pode especificar o uso dos servidores de atualização da Kaspersky Lab, se os servidores personalizados manualmente não estiverem disponíveis.

     b. Na seção **Otimização de uso de E/S de disco** para a tarefa de Atualização do Banco de Dados, é possível configurar o recurso que reduz a carga de trabalho no subsistema de disco:
        - **Diminuir a carga na E/S de disco**

          Esta caixa ativa ou desativa o recurso da otimização de subsistema de disco por meio do armazenamento de arquivos de atualização em uma unidade virtual na RAM.

          Se a caixa de seleção estiver selecionada, esta função será ativada.

          Esta caixa é desmarcada por padrão.
        - **RAM usada para otimização (MB)**

          O tamanho da RAM (em MB) que o aplicativo usa para armazenar arquivos de atualização. O tamanho de RAM padrão é 512 MB. O tamanho de RAM padrão é 400 MB.

     c. Clique no botão **Configurações de conexão** e, na janela **Configurações de conexão** exibida, configure o uso de servidor proxy para conexão com os servidores de atualização da Kaspersky Lab e outros servidores.

- Em **Configurações para atualizações dos módulos de software do aplicativo** para a tarefa Atualizações dos Módulos de Software, é possível especificar quais ações o Kaspersky Embedded Systems Security 2.2 deve executar quando as atualizações dos módulos de software críticas estão disponíveis ou as informações sobre as atualizações planejadas estão disponíveis e é possível especificar também quais ações o Kaspersky Embedded Systems Security 2.2 deve realizar quando as atualizações críticas forem instaladas.
- Especifique o conjunto de atualizações e a pasta de destino na seção **Configurações de Copiar Atualizações** para a tarefa **Copiar Atualizações**.

6. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
7. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa.

> Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

8. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

As configurações de tarefas de grupo definidas recentemente são salvas

Para a tarefa de Reversão da Atualização do Banco de Dados, é possível definir somente configurações de tarefa padrão controladas pelo Kaspersky Security Center nas seções **Notificações** e **Exclusões** do escopo da tarefa. Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

Verificação da integridade de módulos de software

► *Para configurar a tarefa de grupo Atualização dos Módulos de Software:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e seleciona o grupo de administração para o qual deseja configurar as tarefas de aplicativo.
2. No painel de detalhes de um grupo de administração selecionado, abra a guia **Tarefas**.
3. Na lista de tarefas de grupo criadas anteriormente, selecione uma tarefa que deseja configurar. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa na lista de tarefas criadas.
   - Selecione o nome da tarefa na lista de tarefas criadas e clique no link **Configurar tarefa**.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
4. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.

> Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

5. Na seção **Dispositivos**, selecione os dispositivos para os quais você deseja configurar a tarefa de Verificação da integridade de módulos de software.

6. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
7. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa.
8. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

   > Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

9. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

   As configurações de tarefas de grupo definidas recentemente são salvas.

Criando uma tarefa de Verificação por Demanda

► *Para criar uma nova tarefa no Console de Administração do Kaspersky Security Center:*

1. Inicie o assistente de tarefa de uma das seguintes maneiras:
   - Para criar uma tarefa local:
     a. Expanda o nó **Dispositivos gerenciados** na árvore do Servidor de Administração do Kaspersky Security Center e selecione o grupo ao qual o computador protegido pertence.
     b. No painel de detalhes, na guia **Dispositivos**, abra o menu de contexto na linha com informações sobre o computador protegido e selecione **Propriedades**.
     c. Na janela exibida, clique no botão **Adicionar** na seção **Tarefas**.
   - Para criar uma tarefa de grupo:
     a. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo para o qual você deseja criar uma política.
     b. No painel de detalhes, abra o menu de contexto na guia **Tarefas** e selecione **Nova > Tarefa**.
   - Para criar uma tarefa para um conjunto personalizado de computadores, no nó **Seleções de dispositivo** na árvore do Console de Administração do Kaspersky Security Center, selecione **Nova tarefa**.

   A janela do assistente de tarefa é exibida.
2. Na janela **Especificar nome da tarefa**, insira um nome para a tarefa (com menos de 100 caracteres) sem incluir os símbolos **I * < > ? \ / | :)**. É recomendado adicionar o tipo de tarefa ao seu nome (por exemplo, "Verificação por demanda de pastas compartilhadas").
3. Na janela **Tipo de tarefa**, sob o título **Kaspersky Embedded Systems Security 2.2**, selecione a tarefa **Verificação por Demanda** e clique em **Avançar**.
4. Crie um escopo de verificação na janela **Escopo da verificação**.

   > Por padrão, o escopo da verificação inclui áreas críticas do computador. Os escopos da verificação são marcados na tabela com o ícone ☑. Os escopos da verificação excluídos são marcados com o ícone ☐ na tabela.

Você pode alterar o escopo da verificação: adicione escopos, discos, pastas, objetos de rede e arquivos e atribua configurações de segurança específicas para cada escopo adicionado.

- Para excluir todas as áreas críticas da verificação, abra o menu de contexto de cada linha e selecione a opção **Remover escopo**.
- Para incluir um escopo de verificação predefinido, um disco, uma pasta, um objeto de rede ou um arquivo no escopo da verificação:
  a. Clique com o botão direito na tabela **Escopo da verificação** e selecione **Adicionar escopo** ou clique no botão **Adicionar**.
  b. Na janela **Adicionar objetos ao escopo da verificação**, selecione o escopo predefinido na lista **Escopo predefinido**, especifique a unidade do computador, pasta, objeto de rede ou arquivo no computador ou em outro computador da rede e clique no botão **OK**.
- Para excluir subpastas ou arquivos da verificação, selecione a pasta adicionada (disco) na janela **Escopo da verificação** do assistente:
  a. Abra o menu de contexto e selecione opção **Configurar**.
  b. Clique no botão **Configurações** na janela **Nível de segurança**.
  c. Na guia **Geral**, em **Configurações da verificação por demanda**, desmarque as caixas de seleção **Subpastas** e **Subarquivos**.
- Para alterar as configurações de segurança do escopo da verificação:
  a. Abra o menu de contexto do escopo cujas configurações você deseja definir e selecione **Configurar**.
  b. Na janela Configurações da**Verificação por demanda**, selecione um dos níveis de segurança predefinidos ou clique no botão **Configurações** para definir as configurações de segurança manualmente.

  As configurações de segurança são definidas do mesmo modo para a tarefa Proteção de Arquivos em Tempo Real (consulte a seção "Definição manual de configurações de segurança" na página 155).

- Para ignorar objetos incorporados no escopo da verificação adicionado:
  a. Abra o menu de contexto na tabela **Escopo da verificação** e selecione a exclusão **Adicionar**.
  b. Especifique os objetos a serem excluídos: selecione o escopo predefinido na lista **Escopo predefinido**, especifique o disco de computador, a pasta, o objeto de rede ou o arquivo do computador ou em outro computador de rede.
  c. Clique no botão **OK**.

5. Na janela **Opções**, configure o analisador heurístico e a integração com outros componentes:
   - Configure o uso do analisador heurístico (consulte a seção "Usando o Analisador Heurístico" na página 150).
   - Selecione a caixa **Aplicar Zona Confiável** se desejar excluir os objetos descritos na Zona Confiável do Kaspersky Embedded Systems Security 2.2 do escopo da verificação da tarefa.

     Esta caixa de seleção ativa/desativa o uso da zona confiável para uma tarefa.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2

adiciona operações de arquivos de processos confiáveis às exclusões da verificação definidas nas configurações de tarefa.

Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 desconsiderará as operações de arquivo de processos confiáveis ao formar o escopo da proteção para a tarefa de Proteção de Arquivos em Tempo Real.

A caixa de seleção é selecionada por padrão.

- Selecione a caixa **Usar a KSN para verificação** se quiser usar os serviços na nuvem da Kaspersky Security Network para a tarefa.

  Esta caixa ativa/desativa o uso de serviços na nuvem da Kaspersky Security Network (KSN) na tarefa.

  Se a caixa é selecionada, o aplicativo usa os dados de recebidos dos serviços da KSN para garantir um tempo de resposta mais rápido pelo aplicativo para novas ameaças e reduzir a probabilidade de falsos positivos.

  Se a caixa estiver desmarcada, a tarefa de Verificação por Demanda não usará o serviço da KSN.

  A caixa de seleção é selecionada por padrão.

- Para atribuir a prioridade básica **Baixo** ao processo de trabalho onde a tarefa será executada, selecione a caixa de seleção **Executar tarefa em segundo plano** na janela **Opções**.

  A caixa modifica a prioridade da tarefa.

  Se a caixa de seleção estiver selecionada, a prioridade da tarefa no sistema operacional será reduzida. O sistema operacional fornece recursos para a execução da tarefa dependendo da carga da CPU e do sistema de arquivos do computador a partir de outras tarefas e aplicativos do Kaspersky Embedded Systems Security 2.2. Como resultado, o desempenho da tarefa será reduzido durante cargas maiores e será acelerado durante cargas menores.

  Se a caixa de seleção estiver desmarcada, a tarefa será iniciada e executada com a mesma prioridade de outras tarefas do Kaspersky Embedded Systems Security 2.2 e de outros aplicativos. Nesse caso, a velocidade de execução da tarefa será aumentada.

  Esta caixa é desmarcada por padrão.

> Por padrão, os processos de trabalho em que as tarefas do Kaspersky Embedded Systems Security 2.2 são executadas têm a prioridade **Médio** (Normal).

- Para usar a tarefa criada como uma tarefa de Verificação de Áreas Críticas, selecione a caixa **Considerar tarefa como verificação de áreas críticas** na janela **Opções**.

  A caixa de seleção altera a prioridade da tarefa: ativa ou desativa o registro em log do evento de *Verificação de Áreas Críticas* e a atualização do status de proteção do computador. O Kaspersky Security Center avalia a classificação de segurança do computador (computadores) pelos resultados de desempenho de tarefas com o status de *Verificação de Áreas Críticas*. A caixa não está disponível nas propriedades do sistema local e nas tarefas personalizadas do Kaspersky Embedded Systems Security 2.2. Você pode editar esta definição apenas do lado do Kaspersky Security Center.

  Se esta caixa de seleção estiver selecionada, o Servidor de Administração registrará o evento concluído de Verificação de Áreas Críticas e atualizará o status de proteção do computador com base nos resultados da execução da tarefa. A tarefa de verificação possui uma prioridade alta.

Se a caixa estiver desmarcada, a tarefa será executada com uma prioridade baixa.

A caixa de seleção será selecionada por padrão na tarefa de Verificação de áreas críticas.

6. Clique em **Avançar**.
7. Na janela **Programação**, defina um agendamento (consulte a seção "Definição das configurações de programação de inicialização da tarefa" na página 122) para a tarefa.
8. Especifique uma conta de usuário abaixo da qual deseja executar a tarefa e definir o nome de tarefa.
9. Clique em **Finalizar**.

A nova tarefa de Verificação por Demanda será criada para um computador ou um grupo de computadores selecionado.

Configurando uma tarefa de Verificação por Demanda

► *Para configurar uma tarefa existente de Verificação por Demanda, execute as seguintes etapas:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e seleciona o grupo de administração para o qual deseja configurar as tarefas de aplicativo.
2. No painel de detalhes de um grupo de administração selecionado, abra a guia **Tarefas**.
3. Na lista de tarefas de grupo criadas anteriormente, selecione uma tarefa que deseja configurar. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa na lista de tarefas criadas.
   - Selecione o nome da tarefa na lista de tarefas criadas e clique no link **Configurar tarefa**.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
4. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.

   Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

5. Na seção **Configurações**, é possível realizar as ações a seguir:
   a. Na seção **Escopo da verificação**, marque as caixas de seleção ao lado dos recursos do arquivo que deseja incluir no escopo da verificação.
   b. Clique no botão **Configurar** e selecione o nível de segurança.

      Você pode selecionar um dos níveis de segurança predefinidos ou personalizar o nível de segurança manualmente.

   c. Para configurar o nível de segurança manualmente, na janela **Configurações da verificação por demanda**, clique em **Configurações**.
6. Na seção **Opções**, é possível realizar as seguintes ações:
   a. Ativar ou desativar o uso do **Analisador Heurístico** e definir o nível de análise usando o controle deslizante no bloco **Analisador heurístico**.

b. Definir as configurações avançadas (consulte a seção "Criando uma tarefa de Verificação por Demanda" na página 113).

7. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
8. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa.
9. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

   Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

10. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

    As configurações de tarefas de grupo definidas recentemente são salvas.

Atribuindo o status de tarefa de Verificação de Áreas Críticas a uma tarefa de Verificação por Demanda

Por padrão, o Kaspersky Security Center atribui o status *Aviso* ao computador se a tarefa Verificação de Áreas Críticas for executada com menos frequência do que o especificado na configuração de limite de geração de eventos **A verificação das áreas críticas não é realizada há muito tempo** do Kaspersky Embedded Systems Security 2.2.

► *Para configurar a verificação de todos os computadores em um único grupo de administração:*

1. Crie uma tarefa de Verificação por Demanda de grupo.
2. Na janela **Opções** do assistente de tarefas, selecione a caixa **Considerar tarefa como verificação de áreas críticas**. As configurações da tarefa especificadas (o escopo da verificação e as configurações de segurança) serão aplicadas a todos os computadores do grupo. Configure a programação da tarefa.

   É possível marcar a caixa de seleção **Considerar tarefa como verificação de áreas críticas** ao criar a tarefa de Verificação por Demanda para um grupo de computadores ou um conjunto de computadores, e mais tarde, na janela **Propriedades: <nome da tarefa>**.

3. Usar uma política nova ou existente desativa o início programado de tarefas de verificação de sistema (consulte a seção "Configurando a inicialização programada de tarefas locais de sistema" na página 95) nos computadores de grupo.

O Servidor de Administração do Kaspersky Security Center avaliará então o status de segurança do computador protegido e notificará o usuário sobre os resultados da última execução da tarefa com o status da tarefa Verificação de Áreas Críticas, em vez de o fazer com base nos resultados da tarefa do sistema *Verificação de Áreas Críticas*.

Você pode atribuir o status da tarefa *Verificação de Áreas Críticas* às tarefas de grupo de Verificação por Demanda e a tarefas de conjuntos de computadores.

O Console do Aplicativo pode ser usado para visualizar se a tarefa de Verificação por Demanda é uma tarefa de Verificação de Áreas Críticas.

No Console do Aplicativo, a caixa de seleção **Considerar tarefa como verificação de áreas críticas** é exibida nas propriedades da tarefa, mas não pode ser editada.

Verificação de arquivos no armazenamento de nuvem

Sobre arquivos de nuvem

O Kaspersky Embedded Systems Security 2.2 pode interagir com arquivos de nuvem do Microsoft OneDrive. O aplicativo é compatível com o novo recurso de Arquivos Sob Demanda do OneDrive.

> O Kaspersky Embedded Systems Security 2.2 não é compatível com outros armazenamentos de nuvem.

O recurso Arquivos Sob Demanda do OneDrive ajuda você a acessar todos os seus arquivos no OneDrive sem precisar baixar de todos eles e usar espaço de armazenamento no seu dispositivo. Você pode baixar arquivos no seu disco rígido quando precisar.

Quando o recurso de Arquivos Sob Demanda do OneDrive estiver ativo, você verá ícones de status ao lado de cada arquivo na coluna **Status** no Explorador de Arquivos. Cada arquivo tem um dos seguintes status:

Este ícone de status indica que o arquivo *está disponível apenas online*. Os arquivos disponíveis apenas online não estão fisicamente armazenados em seu disco rígido. Você não pode abrir arquivos apenas online quando o seu dispositivo não estiver conectado à Internet.

Este ícone de status indica que um arquivo está *disponível localmente*. Isso acontece quando você abre um arquivo disponível apenas online e o baixa para o seu dispositivo. Você pode abrir um arquivo disponível localmente a qualquer momento, mesmo sem acesso à internet. Para limpar espaço, você pode alterar o arquivo novamente para disponível apenas online.

Este ícone de status indica que um arquivo está *armazenado em seu disco rígido e sempre está disponível*.

Verificação de arquivo de nuvem

O Kaspersky Embedded Systems Security 2.2 só pode verificar arquivos de nuvem armazenados localmente em um computador protegido. Tais arquivos de OneDrive têm o status e . Os arquivos são ignorados durante a verificação, já que não estão fisicamente localizados no computador protegido.

> O Kaspersky Embedded Systems Security 2.2 não baixa automaticamente arquivos da nuvem durante a verificação, mesmo se eles estiverem incluídos no escopo da verificação.

Os arquivos de nuvem são processados por várias tarefas do Kaspersky Embedded Systems Security 2.2 tarefas em vários cenários, dependendo do tipo de tarefa:

- Verificação de arquivos de nuvem em tempo real: você pode adicionar pastas que contêm arquivos de nuvem ao escopo da proteção de tarefa de Proteção de Arquivos em Tempo Real. O arquivo é verificado quando for acessado pelo usuário. Se um arquivo for acessado pelo usuário, ele é baixado, fica localmente disponível e seu status é alterado para . Isso permite que o arquivo seja processado pela tarefa de Proteção de Arquivos em Tempo Real.
- Verificação de arquivos por demanda: você pode adicionar pastas que contêm arquivos de nuvem ao escopo da verificação da tarefa de Verificação por Demanda. A tarefa verifica arquivos com o status e . Se algum arquivo for encontrado no escopo, eles serão ignorados durante a verificação e um evento informativo será registrado no log de tarefas indicando que o arquivo verificado é apenas um marcador de posição para um arquivo de nuvem, e que não existe em uma unidade local.
- Geração e uso de regra de controle do aplicativo: você pode criar regras de permissão e negação para arquivos e usando a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos.

A tarefa de Controle de Inicialização de Aplicativos aplica o princípio de Negação padrão e cria regras para processar e bloquear arquivos de nuvem.

A tarefa de Controle de Inicialização de Aplicativos bloqueia o início de todos os arquivos de nuvem, independentemente do status. Os arquivos não são incluídos no escopo da geração de regra pelo aplicativo, já que não estão fisicamente armazenados em um disco rígido. Já que nenhuma regra de permissão não pode ser criada para tais arquivos, eles ficam sujeitos ao princípio de Negação padrão.

Quando uma ameaça for detectada em um arquivo de nuvem do OneDrive, o aplicativo aplicará a ação especificada nas configurações da tarefa que executa a verificação. Assim, o arquivo pode ser removido, desinfectado, movido para a Quarentena ou gravado em Backup.

As alterações em arquivos locais são sincronizadas com as cópias armazenadas no OneDrive conforme os princípios indicados na documentação relevante do Microsoft OneDrive.

Definindo configurações de diagnóstico de travamento no Kaspersky Security Center

Se um problema ocorrer durante a operação do Kaspersky Embedded Systems Security 2.2 (por exemplo, travamentos do Kaspersky Embedded Systems Security 2.2) e você desejar diagnosticá-lo, é possível ativar a criação de arquivos de rastreamento e o arquivo de despejo do processo do Kaspersky Embedded Systems Security 2.2 e enviar estes arquivos para análise ao Suporte Técnico da Kaspersky Lab.

O Kaspersky Embedded Systems Security 2.2 não envia nenhum arquivo de rastreamento ou de despejo automaticamente. Os dados de diagnóstico só podem ser enviados pelo usuário com as permissões correspondentes.

O Kaspersky Embedded Systems Security 2.2 grava as informações nos arquivos de rastreamento e no arquivo de despejo de modo não criptografado. A pasta onde os arquivos são salvos é selecionada pelo usuário e gerenciada pela configuração do sistema operacional e do Kaspersky Embedded Systems Security 2.2. Você pode configurar permissões de acesso (consulte a seção "Permissões de acesso às funções do Kaspersky Embedded Systems Security 2.2" na página 77) e permitir o acesso a arquivos de log, rastreamento e de despejo apenas para usuários necessários.

► *Definindo configurações de diagnóstico de travamento no Kaspersky Security Center:*

1. No Console de Administração do Kaspersky Security Center, abra a janela **Configurações do aplicativo** (consulte a seção "**Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center**" na página 101).
2. Na guia **Diagnóstico de funcionamento incorreto**, execute as ações seguintes:
   - Se você quiser que o aplicativo grave as informações de depuração no arquivo, marque a caixa

de seleção **Gravar informações de depuração no arquivo de rastreamento**.

- No campo abaixo, especifique a pasta na qual o Kaspersky Embedded Systems Security 2.2 salvará os arquivos de rastreamento.
- Configure o nível de detalhe das informações de depuração.

  Esta lista suspensa permite a seleção do nível de detalhe das informações de depuração que o Kaspersky Embedded Systems Security 2.2 salva no arquivo de rastreamento.

  Você pode selecionar um dos seguintes níveis de detalhe:

  - **Eventos críticos** – O Kaspersky Embedded Systems Security 2.2 salvará apenas as informações sobre eventos críticos no arquivo de rastreamento.
  - **Erros** – O Kaspersky Embedded Systems Security 2.2 salvará as informações sobre eventos críticos e erros no arquivo de rastreamento.
  - **Eventos importantes** – O Kaspersky Embedded Systems Security 2.2 salvará as informações sobre eventos críticos, erros e eventos importantes relacionados ao arquivo de rastreamento.
  - **Eventos informativos** – O Kaspersky Embedded Systems Security 2.2 salvará as informações sobre eventos críticos, erros, eventos importantes e eventos informativos no arquivo de rastreamento.
  - **Todas as informações da depuração** – O Kaspersky Embedded Systems Security 2.2 salvará todas as informações de depuração no arquivo de rastreamento.

  Um representante do Suporte Técnico determina o nível de detalhe que deve ser configurado para solucionar os problemas que ocorram.

  O nível de detalhes padrão é configurado como **Todas as informações da depuração**.

  A lista suspensa estará disponível se a caixa de seleção **Gravar informações de depuração no arquivo de rastreamento** estiver selecionada.

- Especifique o tamanho máximo dos arquivos de rastreamento.
- Especifique os componentes a serem depurados. Os códigos dos componentes devem ser separados por ponto e vírgula. Os códigos diferem entre maiúsculas e minúsculas (consulte a tabela abaixo).

Tabela 27. Códigos de subsistema do Kaspersky Embedded Systems Security 2.2

Código do componente	Nome do componente
*	Todos os componentes.
gui	Subsistema da interface de usuário, snap-in do Kaspersky Embedded Systems Security 2.2 no Console de Gerenciamento da Microsoft.
ak_conn	Subsistema para a integração entre o Agente de rede e o Kaspersky Security Center.
bl	Processo de controle, implementa as tarefas de controle do Kaspersky Embedded Systems Security 2.2.
wp	Processo de trabalho, trata das tarefas de proteção do antivírus.
blgate	Processo de gerenciamento remoto do Kaspersky Embedded Systems Security 2.2.
ods	Subsistema de Verificação por Demanda.

Código do componente	Nome do componente
oas	Subsistema de Proteção de Arquivos em Tempo Real.
qb	Subsistema da Quarentena e do Backup.
scandll	Módulo auxiliar para a verificação do antivírus.
core	Subsistema para a funcionalidade básica do antivírus.
avscan	Subsistema de processamento do antivírus.
avserv	Subsistema para controlar o kernel do antivírus.
prague	Subsistema para funcionalidade básica.
updater	Subsistema de atualização para bancos de dados e módulos do software.
snmp	Subsistema de suporte ao protocolo SNMP.
perfcount	Subsistema do contador de desempenho.

As configurações de rastreamento do snap-in (guia) do Kaspersky Embedded Systems Security 2.2 e do Plug-in de Administração do Kaspersky Embedded Systems Security para o Kaspersky Security Center (ak_conn) serão aplicadas após estes componentes terem sido reiniciados. As configurações de rastreamento do subsistema de suporte de protocolo SNMP (snmp) serão aplicadas após o serviço SNMP ter sido reiniciado. As configurações de rastreamento do subsistema dos contadores de desempenho (perfcount) serão aplicadas após todos os processos que utilizam contadores de desempenho terem sido reiniciados. As configurações de rastreamento para outros subsistemas do Kaspersky Embedded Systems Security 2.2 serão aplicadas assim que as configurações de diagnóstico de travamento forem salvas.

Por padrão, o Kaspersky Embedded Systems Security 2.2 registra informações de depuração para todos os componentes do Kaspersky Embedded Systems Security 2.2.

O campo de inserção estará disponível se a caixa de seleção **Gravar informações de depuração no arquivo de rastreamento** estiver selecionada.

- Se desejar que o aplicativo crie um arquivo de despejo, selecione a caixa **Criar arquivo de despejo**.
  - No campo abaixo especifique a pasta na qual o Kaspersky Embedded Systems Security 2.2 salvará os arquivos de despejo da memória.

3. Clique em **OK**.

As configurações do aplicativo definidas são aplicadas no computador protegido.

Gerenciando programações de tarefas

Você pode configurar a programação de inicialização para tarefas do Kaspersky Embedded Systems Security 2.2 e definir as configurações para executar tarefas pela programação.

Nesta seção

Definição das configurações da programação de inicialização da tarefa

É possível configurar a programação de inicialização de tarefas para o sistema local e tarefas personalizadas no Console do Aplicativo. Você não pode definir a programação de inicialização para tarefas de grupo.

► *Para definir as configurações da programação de inicialização de tarefas, execute as seguintes ações:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e faça o seguinte:
   - Se desejar definir configurações de política, no grupo de computador, selecione **Política > <Nome da política> > <Seção> > Configurar > Gerenciamento de tarefa**.
   - Se quiser definir as configurações do aplicativo de um único computador usando o Kaspersky Security Center, abra a janela **Configurações de tarefa** (consulte a seção "**Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center**" na página 101) no Kaspersky Security Center.

     A janela **Configurações** é exibida.
2. Na janela exibida, na guia **Programação**, marque a caixa de seleção **Executar de acordo com o agendamento**.

   Os campos com as configurações de programação para as tarefas de Verificação por Demanda e de Atualização estarão indisponíveis se a inicialização da programação for bloqueada por uma política do Kaspersky Security Center.
3. Configure a programação de acordo com suas necessidades. Para isso, execute as seguintes ações:

   a. Na lista **Frequência**, selecione um dos seguintes valores:
      - **De hora em hora**, se desejar que a tarefa seja executada nos intervalos de um número especificado de horas; especifique o número de horas no campo **A cada <número> hora(s)**.
      - **Diariamente**, se desejar que a tarefa seja executada nos intervalos de um número especificado de dias; especifique o número de dias no campo **A cada <número> dia(s)**.
      - **Semanalmente**, se desejar que a tarefa seja executada nos intervalos de um número especificado de semanas; especifique o número de semanas no campo **A cada <número> semana(s)**. Especifique os dias da semana em que a tarefa será iniciada (por padrão, a tarefa é executada nas segundas-feiras).
      - **Ao iniciar o aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security 2.2.
      - **Após a atualização do banco de dados do aplicativo**, se desejar que a tarefa seja executada após cada atualização do banco de dados do aplicativo.

   b. Especifique a hora para a primeira inicialização da tarefa no campo **Hora inicial**.

   c. No campo **Data inicial**, especifique a data a partir da qual a programação se aplica.

Após ter especificado a frequência de início da tarefa, a hora da primeira execução, a data a partir da qual se aplica a programação e informações sobre a hora estimada para a próxima execução da tarefa são exibidas na parte superior da janela, no campo **Próxima execução**. Informações atualizadas sobre a hora estimada da próxima execução da tarefa serão exibidas sempre que você abrir a janela **Configurações de tarefa** da guia **Programação**.

O valor **Bloqueado pela política** é exibido no campo **Próxima execução** campo se as configurações de política ativas do Kaspersky Security Center proibirem o início de tarefas programadas do sistema (consulte a seção "Configurando a inicialização programada de tarefas locais de sistema" na página 95).

4. Use a guia **Avançado** para definir as configurações de programação a seguir de acordo com os seus requisitos.
   - Na seção **Configurações de interrupção de tarefa**:
     a. Marque a caixa de seleção **Duração** e insira o número de horas e minutos necessários nos campos à direita para especificar a duração máxima da execução da tarefa.
     b. Marque a caixa de seleção **Pausar de** e insira os valores iniciais e finais do intervalo de tempo nos campos à direita para especificar o intervalo de tempo menor que 24 horas durante o qual a execução da tarefa será pausada.
   - Na seção **Configurações avançadas**:
     a. Marque a caixa de seleção **Cancelar agendamento a partir de** e especifique a data a partir da qual a programação será interrompida.
     b. Marque a caixa de seleção **Executar tarefas ignoradas** para ativar a inicialização de tarefas ignoradas.
     c. Marque a caixa de seleção **Aleatorizar o início da tarefa dentro do intervalo de** e especifique um valor em minutos.
5. Clique no botão **Aplicar** para salvar as configurações de início da tarefa.

Ativando e desativando tarefas programadas

Você pode ativar e desativar tarefas programadas antes ou após a definição das configurações de programação.

► *Para ativar ou desativar a programação de início da tarefa, siga estas etapas:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto no nome de tarefa para a qual deseja configurar a programação de inicialização.
2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é exibida.
3. Na janela exibida na guia **Programação**, faça uma das ações a seguir:
   - Marque a caixa de seleção **Executar de acordo com a programação** se desejar ativar o início da tarefa programada.
   - Desmarque a caixa de seleção **Executar de acordo com a programação** se desejar desativar o início da tarefa programada.

> As definições de programação de início da tarefa configuradas não são excluídas e serão aplicadas no próximo início programado da tarefa.

4. Clique no botão **Aplicar**.

As definições de programação de início da tarefa configuradas são salvas.

Gerenciamento das configurações do aplicativo

Esta seção contém informações sobre como definir as configurações gerais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center.

Neste capítulo

Gerenciando o Kaspersky Embedded Systems Security 2.2 a partir do Kaspersky Security Center

É possível gerenciar de modo centralizado vários computadores com o Kaspersky Embedded Systems Security 2.2 instalado e incluído em um grupo de administração por meio do Plug-in de Administração do Kaspersky Embedded Systems Security. O Kaspersky Security Center também permite que você defina separadamente as configurações de operação de cada computador incluído no grupo de administração.

O *grupo de administração* é criado manualmente no lado do Kaspersky Security Center e inclui vários computadores com o Kaspersky Embedded Systems Security 2.2 instalado, para os quais você deseja definir as mesmas configurações de controle e proteção. Para obter mais detalhes sobre a utilização de grupos de administração, consulte a *Ajuda do Kaspersky Security Center*.

> As configurações do aplicativo para um computador não estão disponíveis se a operação do Kaspersky Embedded Systems Security 2.2 naquele computador for controlada por uma política ativa do Kaspersky Security Center.

O Kaspersky Embedded Systems Security 2.2 pode ser gerenciado a partir do Kaspersky Security Center das seguintes maneiras:

- **Usando políticas do Kaspersky Security Center**. As políticas do Kaspersky Security Center podem ser usadas para definir remotamente as mesmas configurações de proteção para um grupo de computadores. As configurações de tarefa especificadas na política ativa têm prioridade sobre configurações de tarefa definidas localmente no Console do Aplicativo ou remotamente na janela **Propriedades: <Nome do computador>** do Kaspersky Security Center.

  Você pode usar políticas para definir as configurações gerais do aplicativo, as configurações de tarefa de Proteção em Tempo Real, configurações de tarefas de Controle de Atividades Locais, configurações de inicialização de tarefas programadas do sistema e configurações de uso de perfil.
- **Usando tarefas de grupo do Kaspersky Security Center**. As tarefas de grupo do Kaspersky Security Center permitem a definição remota de configurações comuns de tarefas com um período de validade para um grupo de computadores.

- É possível utilizar as tarefas de grupo para ativar o aplicativo, definir configurações da tarefa de Verificação por Demanda, atualizar configurações da tarefa e as configurações da tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos.
- **Usando tarefas para um grupo de dispositivos**. As tarefas para um conjunto de dispositivos permitem a definição remota de configurações de tarefa comuns com um período de execução limitado para computadores que não pertencem a nenhum dos grupos de administração.
- **Usando a janela de propriedades de um único computador**. Na janela **Propriedades: <Nome do computador>**, é possível definir remotamente as configurações de tarefa de um único computador incluído no grupo de administração.
  Você pode definir tanto as configurações gerais do aplicativo como as configurações de todas as tarefas do Kaspersky Embedded Systems Security 2.2 se o computador selecionado não for controlado por uma política ativa do Kaspersky Security Center.

O Kaspersky Security Center possibilita definir configurações de aplicativo, recursos avançados e permite que você trabalhe com logs e notificações. É possível definir essas configurações para um grupo de computadores, bem como para um computador individual.

Definindo as configurações gerais do aplicativo no Kaspersky Security Center

Você pode definir configurações gerais para o Kaspersky Embedded Systems Security 2.2 a partir do Kaspersky Security Center para um grupo de computadores ou para um computador.

Nesta seção

Configuração de escalabilidade e interface no Kaspersky Security Center

O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

► *Para definir as configurações de escalabilidade e a interface do aplicativo, siga estas etapas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra

a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).

- Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

  Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Configurações do aplicativo**, no bloco **Escalabilidade e interface**, clique em **Configurações**.
4. Na janela **Escalabilidade e interface** na guia **Geral**, defina as seguintes configurações:

- Na seção **Configurações de escalabilidade**, defina as configurações que estabelecem o número de processos usados pelo Kaspersky Embedded Systems Security 2.2:
  - **Detectar automaticamente as configurações de escalabilidade**.

    O Kaspersky Embedded Systems Security 2.2 regulará automaticamente o número de processos utilizados.
  - **Definir o número de processos de trabalho manualmente**.

    O Kaspersky Embedded Systems Security 2.2 regulará o número de processos de trabalho ativos de acordo com os valores especificados.

    Este é o valor padrão.
    - **Número máximo de processos ativos.**

      Número máximo de processos que o Kaspersky Embedded Systems Security 2.2 usa. O campo de inserção de dados está disponível se a opção **Definir o número de processos de trabalho manualmente** estiver selecionada.
    - **Número de processos para a Proteção em Tempo Real.**

      O número máximo de processos usados pelos componentes da tarefa de Proteção em Tempo Real. O campo de inserção de dados está disponível se a opção **Definir o número de processos de trabalho manualmente** estiver selecionada.
    - **Número de processos para tarefas de Verificação por Demanda em segundo plano.**

      Número máximo de processos utilizados pelo componente de Verificação por demanda ao executar tarefas de Verificação por Demanda em segundo plano. O campo de inserção de dados está disponível se a opção **Definir o número de processos de trabalho manualmente** estiver selecionada.

  Na seção **Interação com o usuário**, configure a exibição do ícone do aplicativo da bandeja do sistema na área de notificação: desmarque ou selecione a caixa **Exibir o ícone da Bandeja do Sistema na barra de tarefas**.

5. Clique em **OK**.

As configurações de aplicativo definidas são salvas.

Definição das configurações de segurança no Kaspersky Security Center

O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

► *Para definir as configurações de segurança manualmente, siga as etapas a seguir:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Configurações do aplicativo**, clique no botão **Configurações** nas definições de **Segurança e confiabilidade**.
4. Na janela **Configurações de segurança**, defina as seguintes configurações:
   - Na seção **Configurações de confiabilidade**, defina as configurações de recuperação de tarefas do Kaspersky Embedded Systems Security 2.2 quando o aplicativo retornar um erro ou for encerrado.
     - **Executar recuperação da tarefa**

       Esta caixa de seleção ativa ou desativa a recuperação do Kaspersky Embedded Systems Security 2.2 quando houver um erro ou o aplicativo for encerrado.

       Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 recuperará automaticamente as tarefas do Kaspersky Embedded Systems Security 2.2 quando houver um erro ou o aplicativo for encerrado.

       Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 não recuperará automaticamente as tarefas do Kaspersky Embedded Systems Security 2.2 quando houver um erro ou o aplicativo for encerrado.

       A caixa de seleção é selecionada por padrão.
     - **Não recuperar tarefas de Verificação por demanda mais do que (vezes)**

       O número de tentativas de recuperação de uma tarefa de Verificação por Demanda após o Kaspersky Embedded Systems Security 2.2 se recuperar de um erro. O campo de inserção estará disponível se a caixa de seleção **Executar recuperação da tarefa** estiver selecionada.

- Na seção **Ações ao mudar para energia de backup UPS**, especifique as limitações na carga do computador criadas pelo Kaspersky Embedded Systems Security 2.2 após mudar para a energia backup de UPS:
  - **Não iniciar tarefas de verificação programadas**

    Esta caixa de seleção ativa ou desativa a inicialização de uma tarefa de verificação programada após o computador mudar para uma fonte de energia UPS até que o modo de fornecimento de energia padrão seja restaurado.

    Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 não executará as tarefas de verificação programadas após o computador mudar para uma fonte UPS até que o modo de fornecimento de energia padrão seja restaurado.

    Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 executará as tarefas de verificação programadas independentemente do modo de fornecimento de energia.

    A caixa de seleção é selecionada por padrão.
  - **Parar tarefas de verificação atuais**

    A caixa de seleção ativa ou desativa a execução das tarefas de verificação após o computador mudar para uma fonte UPS.

    Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 pausará as tarefas de verificação em execução após o computador mudar para uma fonte UPS.

    Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 continuará as tarefas de verificação em execução após o computador mudar para uma fonte UPS.

    A caixa de seleção é selecionada por padrão.

  O computador muda para uma fonte UPS apenas se o nível de carga da bateria cair para menos de 90%.
- Na seção **Configurações de proteção de senha**, defina uma senha para proteger o acesso às funções do Kaspersky Embedded Systems Security 2.2.

5. Clique em **OK**.

As configurações de escalabilidade e de confiabilidade são salvas.

Definição das configurações de conexão usando o Kaspersky Security Center

O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

As configurações de conexão definidas são usadas para conectar o Kaspersky Embedded Systems Security 2.2 aos servidores de atualização e ativação e durante a integração de aplicativos com os serviços da KSN.

► *Para definir as configurações de conexão, siga as etapas a seguir:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Configurações do aplicativo**, clique no botão **Configurações** no bloco **Servidor proxy**.

   A janela **Configurações de conexão** é aberta.
4. Na janela **Configurações de conexão**, defina as seguintes configurações:
   - Na seção **Configurações do servidor proxy**, selecione as configurações de uso do servidor proxy:
     - **Não usar o servidor proxy**.

       Se esta opção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 conecta-se a serviços da KSN diretamente, sem usar nenhum servidor proxy.
     - **Detectar configurações do servidor proxy automaticamente**.

       Se esta opção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 define automaticamente as configurações para a conexão a serviços da KSN usando o Web Proxy Auto-Discovery Protocol (WPAD).

       Esta opção é selecionada por padrão.
     - **Usar configurações especificadas de servidor proxy**.

       Se esta opção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 se conectará à KSN usando configurações de servidor proxy especificadas manualmente.
     - Endereço IP ou o nome do símbolo do servidor proxy e o número da porta.
     - **Ignorar o servidor proxy para endereços locais**.

       A caixa ativa ou desativa o uso de um servidor proxy ao acessar computadores localizados na mesma rede que o computador com o Kaspersky Embedded Systems Security 2.2 instalado.

       Se esta caixa estiver selecionada, os computadores serão acessados diretamente da rede, que hospeda o computador com o Kaspersky Embedded Systems Security 2.2 instalado. Nenhum servidor proxy é usado.

       Se a caixa estiver desmarcada, o servidor proxy será aplicado para se conectar a computadores locais.

       A caixa de seleção é selecionada por padrão.

- Na seção **Configurações de autenticação do servidor proxy**, especifique as configurações de autenticação:
    - Selecione as configurações de autenticação na lista suspensa.
        - **Não usar autenticação** – a autenticação não é executada. Esse modo é selecionado por padrão.
        - **Usar autenticação NTLM** – a autenticação será executada com o protocolo de autenticação de rede NTLM desenvolvido pela Microsoft.
        - **Usar autenticação NTLM com nome de usuário e senha** – a autenticação será executada usando o nome e a senha através do protocolo de autenticação de rede NTLM desenvolvido pela Microsoft.
        - **Aplicar nome de usuário e senha** – a autenticação é executada com o uso de um nome de usuário e senha.
    - Insira o nome do usuário e a senha, se necessário.
- No bloco **Licenciamento** desmarque ou selecione **Usar o Kaspersky Security Center como servidor proxy ao ativar o aplicativo**.

5. Clique em **OK**.

As configurações de conexão definidas são salvas.

Configurando recursos avançados

É possível configurar recursos avançados do Kaspersky Embedded Systems Security 2.2 a partir do Kaspersky Security Center para um grupo de computadores ou para um único computador.

Nesta seção

Configurar a Zona Confiável no Kaspersky Security Center

Por padrão, a zona confiável é aplicada em políticas e tarefas recém-criadas.

► *Para configurar a Zona Confiável:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Suplementar**, clique no botão **Configurações** no bloco **Zona Confiável**.

   A janela **Zona Confiável** é aberta.
4. Na guia **Exclusões**, especifique os objetos a serem ignorados pelo Kaspersky Embedded Systems Security 2.2 durante a verificação:
   - Para criar exclusões recomendadas, clique no botão **Adicionar exclusões recomendadas**.

     Clicar neste botão permite a extensão da lista de exclusões ao adicionar exclusões recomendadas pela Microsoft, exclusões recomendadas pela Kaspersky Lab.
   - Para importar exclusões, clique no botão **Importar** e, na janela exibida, selecione os arquivos que o Kaspersky Embedded Systems 2.2 considerará como confiáveis.
   - Para especificar manualmente as condições sob as quais um arquivo será considerado confiável, clique no botão **Adicionar**. Na janela exibida, especifique as seguintes configurações:
     - **Objeto a ser verificado**

       Adiciona um arquivo, pasta, disco rígido, ou arquivo de script a uma exclusão.

       Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 ignorará o escopo, arquivo, pasta, disco ou arquivo de script predefinidos enquanto executa a verificação de uso do componente do Kaspersky Embedded Systems Security 2.2 selecionado na seção **Exclusão do escopo de uso**.

       A caixa de seleção é selecionada por padrão.
     - **Objeto a ser detectado**

       Os objetos são excluídos da verificação por meio do nome ou da máscara de nome do objeto detectável. A lista de nomes de objetos detectáveis está disponível no site da Enciclopédia de Vírus.

       Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security

2.2 ignorará os objetos detectáveis especificados durante a verificação.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 detectará todos os objetos especificados no aplicativo por padrão.

Esta caixa é desmarcada por padrão.

- **Exclusão do escopo de uso**

  Nome da tarefa do Kaspersky Embedded Systems Security 2.2 na qual a regra é usada.

- Se necessário, especifique as informações adicionais explicando a exclusão no campo **Comentário**.

5. Na janela **Zona Confiável** na guia **Processos confiáveis** especifique os processos a serem ignorados pelo Kaspersky Embedded Systems Security 2.2 durante a verificação:
   - **Não verificar operações de backup de arquivos**

     A caixa de seleção ativa ou desativa a verificação dos arquivos lidos da operação se tais operações forem executadas pelas ferramentas de Backup instaladas no computador.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 ignorará os arquivos lidos das operações executadas pelas ferramentas de Backup instaladas no computador.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 verificará os arquivos lidos das operações executadas pelas ferramentas de Backup instaladas no computador.

     A caixa de seleção é selecionada por padrão.
   - **Não marcar a atividade dos arquivos dos processos especificados**

     A caixa de seleção ativa ou desativa a verificação da atividade dos arquivos dos processos confiáveis.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 ignorará as operações dos processos confiáveis durante a verificação.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 verificará as operações dos processos confiáveis.

     Esta caixa é desmarcada por padrão.
6. Se necessário, adicione processos cuja atividade de arquivo você não quer verificar (consulte a seção "Adicionar processos confiáveis" na página 133) clicando no botão **Adicionar**.
7. Clique em **OK** na janela **Zona Confiável** para salvar as alterações.

Adicionar processos confiáveis

► *Para adicionar um ou um número de processos à lista de processos confiáveis:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações

do aplicativo do Kaspersky Security Center" na página 101).

> Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Suplementar**, clique no botão **Configurações** no bloco **Zona Confiável**.

   A janela **Zona Confiável** é aberta.
4. Na guia **Processos confiáveis**, selecione a caixa **Não verificar a atividade dos arquivos dos processos especificados**.
5. Clique no botão **Adicionar**.
6. A partir do menu de contexto do botão, selecione uma das seguintes opções:
   - **Múltiplos processos**.

     Na janela **Adição de processos confiáveis** que se abre, configure o seguinte:

     a. **Use o caminho inteiro do processo no disco para saber se é confiável**

        Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 usará o caminho completo até a pasta para determinar o status de confiança do processo.

        Se a caixa de seleção for desmarcada, o caminho para o arquivo não é considerado como um critério para determinar o status de confiança do processo.

        A caixa de seleção é selecionada por padrão.

     b. **Use o hash de arquivo do processo para considerá-lo como confiável**.

        Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 usará o hash do arquivo selecionado para determinar o status de confiança do processo.

        Se a caixa de seleção for desmarcada, o hash do arquivo não será considerado como um critério para determinar o status de confiança do processo.

        A caixa de seleção é selecionada por padrão.

     c. Clique no **Procurar** para adicionar dados baseados em processos executáveis.

     d. Selecione um outro arquivo executável na janela que se abre.

     > É possível adicionar apenas um arquivo executável por vez. Repita as etapas c-d para adicionar outros arquivos executáveis.

     e. Clique no botão **Processos** para adicionar dados baseados em processos em execução.

     f. Selecione processos na janela que se abre. Para selecionar múltiplos processos, pressione e segure o botão **CTRL** ao selecionar.

     g. Clique em **OK**.

É obrigatório que a conta em que a tarefa Proteção de Arquivos em Tempo Real for executada tenha direitos de administrador no computador com o Kaspersky Embedded Systems Security 2.2 instalado para que seja possível visualizar a lista de processos ativos. Você pode ordenar processos na lista de processos ativos por nome de arquivo, PID ou caminho para o arquivo executável do processo no computador local. Note que é possível selecionar processos em execução clicando no botão **Processos** usando apenas o Console do Aplicativo em um computador local, ou nas configurações do host especificado por meio do Kaspersky Security Center.

- **Um processo baseado no nome e no caminho.**

  Na janela **Adicionar processo confiável manualmente** que se abre, configure o seguinte:

  a. Insira um caminho para o arquivo executável (inclusive o nome do arquivo).

  b. Clique em **OK**.

- **Um processo baseado nas propriedades do objeto.**

  Na janela **Adicionar processo confiável** que se abre, configure o seguinte:

  a. Clique no botão **Procurar** e selecione um processo.

  b. **Use o caminho inteiro do processo no disco para saber se é confiável**

  Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 usará o caminho completo até a pasta para determinar o status de confiança do processo.

  Se a caixa de seleção for desmarcada, o caminho para o arquivo não é considerado como um critério para determinar o status de confiança do processo.

  A caixa de seleção é selecionada por padrão.

  c. **Use o hash de arquivo do processo para saber se é confiável**.

  Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 usará o hash do arquivo selecionado para determinar o status de confiança do processo.

  Se a caixa de seleção for desmarcada, o hash do arquivo não será considerado como um critério para determinar o status de confiança do processo.

  A caixa de seleção é selecionada por padrão.

  d. Clique em **OK**.

  Para adicionar o processo selecionado à lista de processos confiáveis, pelo menos um critério de confiança deve ser selecionado.

7. Na janela **Adicionar processo confiável**, clique no botão **OK**.

O arquivo ou processo selecionado será adicionado à lista de processos confiáveis na janela **Zona Confiável**.

Aplicar a máscara de não vírus

A máscara de não vírus permite ignorar arquivos de software e recursos da web legítimos, que podem ser considerados perigosos, durante a verificação. A máscara afeta as seguintes tarefas:

- Proteção de Arquivos em Tempo Real.
- Verificação por Demanda.

Se a máscara não for adicionada à lista de exclusões, o Kaspersky Embedded Systems Security 2.2 aplicará as ações especificadas nas configurações de tarefa para os recursos de software ou da web sob esta categoria.

► *Para aplicar a máscara de não vírus:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

     > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Suplementar**, clique no botão **Configurações** no bloco **Zona Confiável**.

   A janela **Zona Confiável** é aberta.
4. Na guia **Exclusões**, role pela lista e selecione a linha com o valor **não vírus:*** se a caixa estiver desmarcada.
5. Clique em **OK**.

A nova configuração é aplicada.

Verificação de unidades removíveis

É possível configurar a verificação de unidades removíveis conectadas ao computador protegido por meio da porta USB.

O Kaspersky Embedded Systems Security 2.2 verifica uma unidade removível usando a tarefa de Verificação por Demanda. O aplicativo cria uma nova tarefa de Verificação por Demanda automaticamente quando a unidade removível é conectada e a exclui após a verificação ser concluída. A tarefa criada é executada com o nível de segurança predefinido para a verificação de unidade removível. Não é possível definir as configurações da tarefa temporária de Verificação por Demanda.

> O Kaspersky Embedded Systems Security 2.2 verifica as unidades USB removíveis conectadas quando elas são registradas como dispositivos de armazenamento USB em massa no sistema operacional. O aplicativo não verifica uma unidade removível se a conexão for bloqueada pela tarefa de Controle de Dispositivos. O aplicativo não verifica os dispositivos móveis conectados por MTP.

O Kaspersky Embedded Systems Security 2.2 permite o acesso a unidades removíveis durante a verificação.

Os resultados para cada unidade removível estão disponíveis no log para a tarefa de Verificação por Demanda criada após a conexão da unidade removível.

É possível alterar as configurações do componente de Verificação de unidades removíveis (consulte a tabela abaixo).

Tabela 28. Configurações de verificação de unidades removíveis

Configuração	Valor padrão	Descrição
Verificar unidades removíveis na conexão via USB	A caixa de seleção é desmarcada	É possível ligar e desligar a verificação de unidade removível após a conexão via USB com o computador protegido.
Verificar unidades removíveis se o volume de dados armazenados não exceder (MB):	1024 MB	É possível reduzir o escopo do componente configurando o volume máximo de dados na unidade verificada. O Kaspersky Embedded Systems Security 2.2 não realiza a verificação da unidade removível se o volume de dados armazenados exceder o valor especificado.
Verificação com nível de segurança	Proteção máxima	É possível configurar as tarefas criadas de Verificação por Demanda selecionando um dos três níveis de segurança: • Proteção máxima • Recomendado • Desempenho máximo O algoritmo utilizado quando objetos infectados, possivelmente infectados e outros são detectados, bem como as outras configurações de verificação para cada nível de segurança, correspondem àqueles predefinidos nas tarefas de Verificação por Demanda.

► *Para configurar a verificação de unidades removíveis na conexão, realize as seguintes ações:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Suplementar**, clique em **Configurações** no bloco **Verificação de unidades removíveis**.

   A janela **Verificação de unidades removíveis** é exibida.

4. Na seção **Verificação na conexão**, faça o seguinte:

   - Marque a caixa de seleção **Verificar unidades removíveis na conexão via USB** se desejar que o Kaspersky Embedded Systems Security 2.2 verifique automaticamente as unidades removíveis quando elas forem conectadas.
   - Se necessário, selecione **Verificar unidades removíveis se o volume de dados armazenados não exceder (MB)** e especifique o valor máximo no campo à direita.
   - Na lista suspensa **Verificação com nível de segurança**, especifique o nível de segurança com as configurações exigidas para a verificação de unidades removíveis.

5. Clique em **OK**.

   As configurações específicas são salvas e aplicadas.

Configurando permissões de acesso no Kaspersky Security Center

Você pode configurar permissões de acesso para gerenciar o aplicativo e o Kaspersky Security Service no Kaspersky Security Center para um grupo de computadores ou para um computador separado.

> O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

► *Para acessar permissões para gerenciar o aplicativo e o Kaspersky Security Service:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Suplementar**, execute as seguintes ações:

   - Para configurar permissões de acesso para gerenciar o Kaspersky Embedded Systems Security 2.2 para um usuário ou grupo de usuários, na seção **Permissões de acesso do usuário**

para gerenciamento do aplicativo, clique no botão **Configurações**.

- Para configurar permissões de acesso para gerenciar o Kaspersky Security Service para um usuário ou grupo de usuários, na seção **Permissões de acesso do usuário para gerenciamento do Security Service**, clique no botão **Configurações**.

4. Na janela que se abre, configure os privilégios de acesso (consulte a seção "Permissões de acesso às funções do Kaspersky Embedded Systems Security 2.2" na página 77) segundo as suas necessidades.

As configurações especificadas são salvas.

Definindo as configurações de Quarentena e de Backup no Kaspersky Security Center

O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

► *Para definir as configurações gerais do Backup no Kaspersky Security Center:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Suplementar**, clique no botão **Configurações** no bloco **Armazenamentos**.
4. Use a guia **Backup** da janela de configurações **Armazenamentos** para especificar as configurações de **Backup** que se seguem:
   - Para especificar a **Pasta de backup**, use o campo **Pasta de backup** para selecionar a pasta requerida na unidade local do computador protegido, ou insira o caminho completo.
   - Para configurar o tamanho máximo do **Backup**, selecione a caixa de seleção **Tamanho máximo do backup (MB)** e especifique o valor relevante em megabytes no campo de inserção de dados.
   - Para configurar o limite de espaço disponível no Backup, configure o valor da configuração **Tamanho máximo do backup (MB)**, selecione a caixa **Valor limite de espaço disponível (MB)** e especifique o valor mínimo de espaço disponível na pasta do **Backup** em megabytes.

- Para especificar uma pasta para objetos restaurados, selecione a pasta relevante em uma unidade local do computador protegido na seção Configurações de restauração ou insira o nome da pasta e o caminho completo para a pastas no campo **Pasta destino para a restauração de objetos**.

5. Na janela de configurações **Armazenamentos** na guia **Quarentena**, defina as seguintes configurações da **Quarentena**:
   - Para alterar a pasta de armazenamento da **Quarentena**, no campo de inserção de dados **Quarentena**, especifique o caminho completo para a pasta na unidade local do computador protegido.
   - Para configurar o tamanho máximo da **Quarentena**, selecione a caixa **Tamanho máximo da Quarentena (MB)** e especifique o valor desse parâmetro em megabytes no campo de inserção.
   - Para configurar o volume mínimo de espaço disponível na **Quarentena**, selecione a caixa **Tamanho máximo da Quarentena (MB)** e a caixa **Valor limite de espaço disponível (MB)** e, em seguida, especifique o valor desse parâmetro em megabytes no campo de inserção.
   - Para alterar a pasta onde os objetos são restaurados a partir da Quarentena, no campo de inserção **Pasta destino para a restauração de objetos**, especifique o caminho completo para a pasta na unidade local do computador protegido.
6. Clique em **OK**.

As configurações de Quarentena e Backup definidas são salvas.

Configurações de logs e notificações

O Console de Administração do Kaspersky Security Center pode ser usado para configurar notificações para administradores e usuários sobre os seguintes eventos relacionados ao Kaspersky Embedded Systems Security 2.2 e ao status de proteção de antivírus no computador protegido:

- O administrador pode receber informações sobre eventos de tipos selecionados;
- Os usuários de LAN que acessam o computador protegido e os usuários do computador terminal podem receber informações sobre eventos do tipo *Objeto detectado*.

As notificações sobre os eventos do Kaspersky Embedded Systems Security 2.2 podem ser configuradas para um único computador usando a janela **Propriedades: <Nome do computador>** do computador selecionado, ou para um grupo de computadores na janela **Propriedades: <Nome da política>** do grupo de administração selecionado.

Na guia **Eventos** ou na janela **Configurações de notificação**, você pode configurar os seguintes tipos de notificações:

- As notificações do administrador sobre eventos dos tipos selecionados podem ser configuradas na guia **Eventos** (a guia padrão do aplicativo Kaspersky Security Center). Para obter mais detalhes sobre os métodos de notificação, consulte a *Ajuda do Kaspersky Security Center*.
- As notificações de administrador e usuário podem ser configuradas usando a janela **Configurações de notificação**.

> O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

Você pode configurar notificações para alguns tipos de eventos somente na janela ou na guia; você pode usar tanto a janela quanto a guia para configurar notificações para outros tipos de eventos.

Se você configurar notificações sobre eventos do mesmo tipo usando o mesmo modo na guia **Eventos** e na janela **Configurações de notificação**, o administrador do sistema receberá notificações desses eventos duas vezes, mas no mesmo modo.

Nesta seção

Definição de configurações de log

O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

► *Para configurar os logs do Kaspersky Embedded Systems Security 2.2, execute as seguintes etapas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

     Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Logs e notificações**, clique no botão **Configurações** no bloco **Logs de tarefas**.
4. Na janela **Configurações de notificações**, defina as seguintes configurações do Kaspersky Embedded Systems Security 2.2 de acordo com seus requisitos:
   - Configure o nível de detalhe de eventos em logs. Para isso, execute as seguintes ações:
     a. Na lista **Componente**, selecione o componente do Kaspersky Embedded Systems Security 2.2 para o qual você deseja configurar o nível de detalhe.
     b. Para configurar o nível de detalhes nos logs de tarefa e no log de auditoria do sistema

para o componente selecionado, selecione o nível que deseja em **Nível de importância**.

- Para alterar a localização padrão para logs, especifique o caminho completo para a pasta ou clique no botão **Procurar** para selecioná-la.
- Especifique o número de dias em que os logs de tarefa serão armazenados.
- Especifique o número de dias em que as informações exibidas no nó **Log de auditoria do sistema** serão armazenadas.

5. Clique em **OK**.

As configurações de log definidas são salvas.

Log de segurança

O Kaspersky Embedded Systems Security 2.2 mantém um log de eventos associados a violações de segurança ou tentativas de violação no computador protegido. Os eventos a seguir são registrados nesse log:

- Eventos de Prevenção de Exploits.
- Eventos críticos de Inspeção do Log.
- Eventos críticos que indicam uma tentativa de violação de segurança (para as tarefas de Proteção do Computador em Tempo Real, Verificação por Demanda, Monitor de Integridade de Arquivos, Controle de Inicialização de Aplicativos e Controle de Dispositivos).

Você pode limpar o Log de segurança e também o Log de auditoria do sistema. Além disso, o Kaspersky Embedded Systems Security 2.2 registra eventos de auditoria do sistema relativos à exclusão do Log de segurança.

Definições das configurações de integração SIEM

Para reduzir a carga nos dispositivos de baixo desempenho e reduzir o risco de degradação do sistema como resultado de maiores volumes de logs de aplicativo, é possível configurar a publicação de eventos de auditoria e de desempenho de tarefa para o *servidor syslog* por meio do protocolo Syslog.

Um servidor syslog é um servidor externo para eventos de agregação (SIEM). Ele coleta e analisa eventos recebidos e também executa outras ações de gerenciamento de logs.

É possível usar a integração SIEM de duas maneiras:

- Eventos duplicados no servidor syslog: este modo prescreve que todos os eventos de realização de tarefa cuja publicação esteja definida nas configurações de logs bem como todos os eventos de auditoria do sistema continuem a ser armazenados no computador local mesmo após terem sido enviados ao SIEM.

  Recomenda-se que esse modo seja utilizado para reduzir ao máximo a carga no computador protegido.
- Excluir cópias locais de eventos: este modo prescreve que todos os eventos registrados durante a operação do aplicativo e publicados no SIEM serão excluídos do computador local.

  > O aplicativo nunca exclui versões locais do log de segurança.

O Kaspersky Embedded Systems Security 2.2 pode converter eventos em logs de aplicativo em formatos compatíveis com o servidor syslog para que esses eventos possam ser transmitidos e reconhecidos com sucesso pelo SIEM. O aplicativo é compatível com a conversão para um formato de dados estruturados e para o formato JSON.

Para reduzir o risco de transmissão malsucedida de eventos ao SIEM, é possível definir as configurações para conectar ao servidor syslog de espelhamento.

Um servidor syslog de espelhamento adicional para o qual o aplicativo se alterna automaticamente se a conexão ao servidor principal syslog estiver indisponível ou se o servidor principal não puder ser utilizado.

Por padrão, a integração SIEM não é utilizada. É possível ativar e desativar a integração SIEM e definir as configurações de funcionalidade (consulte a tabela abaixo).

Tabela 29. Configurações de integração SIEM

Configuração	Valor padrão	Descrição
Enviar eventos para um servidor syslog remoto pelo protocolo syslog	Não aplicado	É possível ativar ou desativar a integração SIEM marcando ou desmarcando a caixa de seleção, respectivamente.
Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto	Não aplicado	É possível definir as configurações para armazenar as cópias locais dos logs após eles terem sido enviados ao SIEM marcando ou desmarcando a caixa de seleção.
Formato dos eventos	Dados estruturados	É possível selecionar um de dois formatos nos quais o aplicativo converte seus eventos antes de enviá-los ao servidor syslog para um melhor reconhecimento desses eventos pelo SIEM.
Protocolo de conexão	TCP	Você pode usar a lista suspensa para configurar a conexão ao servidor syslog principal via protocolos UDP ou TCP; ao servidor syslog de espelhamento pelo protocolo TCP.
Configurações de conexão do servidor syslog principal	Endereço IP: 127.0.0.1 Porta: 514	Você pode usar os campos apropriados para configurar o endereço IP e a porta usados para conectar-se ao servidor syslog principal. É possível especificar o endereço IP somente no formato IPv4.
Usar o servidor syslog de espelhamento se o servidor principal não estiver acessível	Não aplicado	É possível usar a caixa de seleção para ativar ou desativar o uso de um servidor syslog refletido.
Configurações de conexão do servidor syslog de espelhamento	Endereço IP: 127.0.0.1 Porta: 514	Você pode usar os campos apropriados para configurar o endereço IP e a porta usados para conectar-se ao servidor syslog principal. É possível especificar o endereço IP somente no formato IPv4.

► *Para definir as configurações de integração SIEM:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas**

e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).

- Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

> Se um dispositivo estiver sendo gerenciado por uma política ativa do Kaspersky Security Center e essa política bloquear alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Logs e notificações**, clique no botão **Configurações** no bloco **Logs de tarefa**.

   A janela **Configurações de logs e notificações** é aberta.
4. Selecione a guia **Integração SIEM**.
5. Na seção **Configurações de integração**, marque a caixa de seleção **Enviar eventos para um servidor syslog remoto pelo protocolo syslog**.

   A caixa de seleção ativa ou desativa a funcionalidade de envio de eventos publicados a um servidor syslog externo.

   Se a caixa de seleção for selecionada, o aplicativo enviará eventos publicados ao SIEM de acordo com as configurações de integração SIEM definidas.

   Se a caixa de seleção for desmarcada, o aplicativo não executará a integração SIEM. Não é possível definir as configurações de integração SIEM se a caixa de seleção for desmarcada.

   Esta caixa é desmarcada por padrão.
6. Se necessário, na seção **Configurações de integração**, marque a caixa de seleção **Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto**.

   A caixa de seleção ativa ou desativa a exclusão de cópias locais de logs quando eles são enviados para o SIEM.

   Se a caixa de seleção for marcada, o aplicativo exclui cópias locais de eventos depois que eles tiverem sido publicados com sucesso no SIEM. Este modo é recomendado em computadores com desempenho limitado.

   Se a caixa de seleção for desmarcada, o aplicativo apenas enviará os eventos para o SIEM. As cópias de logs continuam sendo armazenadas localmente.

   Esta caixa é desmarcada por padrão.

   > O status da caixa de seleção **Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto** não afeta as configurações de armazenamento de eventos do log de segurança: o aplicativo nunca exclui automaticamente os eventos de log de segurança.
7. Na seção **Formato dos eventos**, especifique o formato para o qual deseja converter eventos de operação do aplicativo para que sejam enviados ao SIEM.

   Por padrão, o aplicativo converte-os em um formato de dados estruturados.
8. Na seção **Configurações de conexão**:
   - Especifique o protocolo de conexão SIEM.
   - Especifique as configurações para a conexão com o servidor syslog principal.

É possível especificar um endereço IP somente no formato IPv4.

- Se necessário, marque a caixa de seleção **Usar o servidor syslog de espelhamento se o servidor principal não estiver acessível** se desejar que o aplicativo use outras configurações de conexão quando não for possível enviar eventos para o servidor syslog principal.
  - Especifique as seguintes configurações para conectar ao servidor syslog de espelhamento: **Endereço IP** e **Porta**.

    Os campos **endereço IP** e **Porta** do servidor syslog de espelhamento não poderão ser editados se a caixa de seleção **Usar o servidor syslog de espelhamento se o servidor principal não estiver acessível** estiver desmarcada.

    É possível especificar um endereço IP somente no formato IPv4.

9. Clique em **OK**.

As configurações da integração SIEM definidas serão aplicadas.

Definição de configurações de notificação

► *Para configurar as notificações do Kaspersky Embedded Systems Security 2.2, execute as seguintes etapas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Logs e notificações**, clique no botão **Configurações** no bloco **Notificações de evento**.
4. Na janela **Configurações de notificação**, defina as seguintes configurações do Kaspersky Embedded Systems Security 2.2 de acordo com seus requisitos:
   - Na lista **Configurações de notificações** selecione o tipo da notificação cujas configurações você deseja definir.
   - Na seção **Notificar usuários** configure o método de notificação de usuário. Se necessário, insira o texto da mensagem de notificação.
   - Na seção **Notificar administradores** configure o método de notificação de administrador. Se necessário, insira o texto da mensagem de notificação. Se necessário, defina configurações adicionais de notificação clicando no botão **Configurações**.
   - Na seção **Limites de geração de evento**, especifique os intervalos de tempo após os quais o Kaspersky Embedded Systems Security 2.2 registra os eventos *O banco de dados do aplicativo está*

desatualizado, O banco de dados do aplicativo está muito desatualizado e a *verificação de áreas críticas não é realizada há muito tempo*.

- **O banco de dados do aplicativo está desatualizado (dias)**

  O número de dias decorridos desde a última Atualização do banco de dados.

  O valor padrão é 7 dias.

- **O banco de dados do aplicativo está muito desatualizado (dias)**

  O número de dias decorridos desde a última Atualização do banco de dados.

  O valor padrão é 14 dias.

- **A Verificação de áreas críticas não é executada há muito tempo (dias)**

  O número de dias após a última Verificação de áreas críticas concluída com êxito.

  O valor padrão é 30 dias.

5. Clique em **OK**.

As configurações de notificação definidas são salvas.

Configuração de interações com o Servidor de Administração

► *Para escolher os tipos de objetos sobre os quais o Kaspersky Embedded Systems Security 2.2 envia informações ao Servidor de Administração do Kaspersky Security Center, faça o seguinte:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Logs e notificações**, clique no botão **Configurações** no bloco **Interação com o Servidor de Administração**.

   A janela **Listas da rede do Servidor de administração** é exibida.
4. Na janela **Listas da rede do Servidor de administração**, escolha os tipos de objetos sobre os quais o Kaspersky Embedded Systems Security 2.2 enviará informações ao Servidor de Administração do Kaspersky Security Center:
   - Objetos em Quarentena.
   - Objetos em Backup.
5. Clique em **OK**.

   O Kaspersky Embedded Systems Security 2.2 enviará informações sobre os tipos de objetos selecionados para o Servidor de Administração.

Proteção do Computador em Tempo Real

Esta seção fornece informações sobre componentes Proteção do computador em tempo real: Proteção de Arquivos em Tempo Real, Uso da KSN e Prevenção de Exploits. Esta seção também fornece instruções sobre como configurar tarefas de Proteção em Tempo Real e gerenciar as configurações de segurança de um computador protegido.

Neste capítulo

Proteção de Arquivos em Tempo Real

Esta seção contém informações sobre a tarefa de Proteção de Arquivos em Tempo Real e como configurá-la.

Nesta seção

Sobre a tarefa de Proteção de Arquivos em Tempo Real

Quando a tarefa de Proteção de Arquivos em Tempo Real é executada, o Kaspersky Embedded Systems Security 2.2 verifica os seguintes objetos do computador protegido quando eles são acessados:

- Arquivos.
- Fluxos alternativos do sistema de arquivos (fluxos NTFS).
- Registro mestre de inicialização e setores de inicialização nos discos rígidos locais e dispositivos externos.
- Arquivos de contêiner do Windows Server® 2016 e do Windows Server 2019.

Quando um aplicativo grava um arquivo em um computador ou lê um arquivo a partir dele, o Kaspersky Embedded Systems Security 2.2 intercepta esse arquivo, verifica se existem ameaças e, se uma ameaça for detectada, executa uma ação padrão ou uma ação especificada: tenta desinfectá-lo, coloca-o na Quarentena ou apenas o exclui. O Kaspersky Embedded Systems Security 2.2 retornará o arquivo ao aplicativo se ele não estiver infectado ou se tiver sido desinfectado com êxito.

O Kaspersky Embedded Systems Security 2.2 intercepta operações de arquivos executadas em contêineres do Windows Server 2016 e Windows Server 2019.

Um contêiner é um ambiente isolado que permite que aplicativos sejam executados sem interação direta com o sistema operacional. Se o contêiner estiver localizado no escopo da proteção da tarefa, o Kaspersky Embedded Systems Security 2.2 verifica os arquivos do contêiner que estiverem sendo acessados pelos usuários para ameaças de computador. Quando uma ameaça for detectada, o aplicativo tenta desinfectar o contêiner. Se a tentativa for bem-sucedida, o contêiner continua funcionando; se a desinfecção falhar, o contêiner é fechado.

O Kaspersky Embedded Systems Security 2.2 também detecta malware em processos executados sob o Subsistema Windows para Linux®. Para tais processos, a tarefa de Proteção de Arquivos em Tempo Real aplica a ação definida pela configuração atual.

Definindo as configurações de tarefa de Proteção de Arquivos em Tempo Real

Por padrão, a tarefa do sistema de Proteção de Arquivos em Tempo Real usa as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Tabela 30. Configurações padrão da tarefa de Proteção de arquivos em tempo real

Configuração	Valor padrão	Descrição
Escopo da proteção	O computador inteiro, excluindo unidades virtuais.	Você pode limitar o escopo da proteção.
Nível de segurança	Configurações comuns para todo o escopo da proteção; corresponde ao nível de segurança **Recomendado**.	Para os nós selecionados na árvore de recursos de arquivos do computador, você pode: • Aplicar outro nível de segurança predefinido. • Editar o nível de segurança manualmente. • Salvar as configurações de segurança do nó selecionado como um modelo para uso posterior.
Modo de proteção dos objetos	Ao acessar e modificar.	Você pode selecionar o modo de proteção, ou seja, definir o tipo de acesso usado pelo Kaspersky Embedded Systems Security 2.2 para verificar objetos.
Analisador Heurístico	O nível de segurança **Médio** é aplicado.	É possível ativar ou desativar o Analisador Heurístico, e configurar o nível de análise.
Aplicar Zona Confiável	Aplicada.	Lista geral de exclusões que podem ser usadas em tarefas selecionadas.
Usar a KSN para proteção	Aplicada.	Você pode melhorar a proteção do seu computador usando a infraestrutura dos serviços na nuvem da Kaspersky Security Network (disponível se a Declaração da KSN for aceita).
Programação de inicialização de tarefa	Na inicialização do aplicativo.	Você pode configurar a programação de inicialização de tarefa.

► *Para configurar as definições da tarefa de Proteção de Arquivos em Tempo Real, siga as etapas a seguir:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Proteção de Arquivos em Tempo Real** clique no botão **Configurações** no bloco **Proteção de Arquivos em Tempo Real**.

   A janela **Proteção de arquivos em tempo real** é aberta.
4. Defina as seguintes configurações da tarefa:
   - Na guia **Geral**:
     - O modo de proteção (consulte a seção "Selecionando o modo de proteção" na página 150)
     - Usando o Analisador Heurístico (na página150)
     - Configurações de integração com outros componentes do Kaspersky Embedded Systems Security 2.2.
   - Na guia **Gerenciamento da tarefa**:
     - Configurações de inicialização da tarefa (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 122).
5. Selecione a guia **Escopo da proteção** e faça o seguinte:
   - Clique no botão **Adicionar** ou **Editar** para editar o escopo da proteção (consulte a seção "Escopo da proteção da tarefa de Proteção de Arquivos em Tempo Real" na página 152).
     - Na janela exibida, escolha o que você deseja incluir no escopo da proteção da tarefa:
       - **Escopo predefinido**
       - **Disco, pasta ou local da rede**
       - **Arquivo**
     - Selecione um dos níveis de segurança predefinidos (consulte a seção "Seleção de níveis de segurança predefinidos" na página 153) ou defina manualmente as configurações de proteção (consulte a seção "Definição manual de configuração de segurança" na página 155).
6. Clique em **OK** na janela **Proteção de arquivos em tempo real**.

O Kaspersky Embedded Systems 2.2 aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora quando as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de tarefas.

Usando o Analisador Heurístico

Você pode usar o Analisador Heurístico e configurar o nível da análise das tarefas do Kaspersky Embedded Systems Security 2.2.

► *Para configurar o Analisador Heurístico:*

1. Abra as configurações do aplicativo (consulte a seção "Gerenciando o Kaspersky Embedded Systems Security 2.2 a partir do Kaspersky Security Center" na página 125) ou as configurações de política (consulte a seção "Configurando políticas" na página 90), para as quais deseja configurar o Analisador Heurístico.
2. Desmarque ou selecione a caixa **Usar o analisador heurístico**.

   Esta caixa ativa/desativa o analisador heurístico durante a verificação do objeto.

   Se a caixa de seleção estiver selecionada, o Analisador Heurístico será ativado.

   Se a caixa de seleção estiver desmarcada, o Analisador Heurístico será desativado.

   A caixa de seleção é selecionada por padrão.
3. Se necessário, ajuste o nível da análise usando o controle deslizante.

   O controle deslizante permite o ajuste do nível de análise heurística. O nível de intensidade da verificação define o equilíbrio entre a profundidade das pesquisas de ameaças, a carga sobre os recursos do sistema operacional e o tempo necessário para a verificação.

   Estão disponíveis os seguintes níveis de intensidade da verificação:

   - **Superficial**. O analisador heurístico executa menos operações encontradas nos arquivos executáveis. A probabilidade de detectar ameaças nesse modo é um pouco menor. A verificação é mais rápida e utiliza menos recursos.
   - **Médio**. O Analisador Heurístico executa a quantidade de instruções encontradas nos arquivos executáveis recomendada pelos especialistas da Kaspersky Lab.

     Este nível é selecionado por padrão.
   - **Profundo**. O analisador heurístico executa mais operações encontradas nos arquivos executáveis. De certa forma, a probabilidade de detectar ameaças nesse modo é maior. A verificação esgota mais recursos do sistema, leva mais tempo e pode causar um número mais alto de alarmes falsos.

     O controle deslizante estará disponível se a caixa de seleção **Usar o Analisador Heurístico** estiver selecionada.
4. Clique em **OK**.

As configurações de tarefa definidas são aplicadas imediatamente à tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

Selecionando o modo de proteção

Na tarefa Proteção de Arquivos em Tempo Real, o modo de proteção pode ser selecionado. A seção **Modo de proteção dos objetos** permite a especificação do tipo de acesso aos objetos nos quais o Kaspersky Embedded Systems Security 2.2 deve realizar a verificação.

A configuração **Modo de proteção dos objetos** tem o valor comum para o escopo da proteção inteiro especificado na tarefa. Você não pode especificar valores diferentes para a configuração de nós individuais dentro do escopo da proteção.

► *Para selecionar o modo de proteção:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Proteção do Computador em Tempo Real** clique no botão **Configurações** no bloco **Proteção de arquivos em tempo real**.

   A janela **Proteção de arquivos em tempo real** é aberta.
4. Na janela exibida, abra a guia **Geral** e selecione o modo de proteção que deseja definir:
   - **Modo inteligente**

     O Kaspersky Embedded Systems Security 2.2 seleciona objetos a serem verificados de maneira independente. O objeto é verificado ao ser aberto e novamente depois de ser salvo, caso tenha sido modificado. Se várias chamadas ao objeto foram feitas pelo processo enquanto ele estava em execução e se o processo o modificou, o Kaspersky Embedded Systems Security 2.2 verifica o objeto novamente somente após o objeto ter sido salvo pelo processo pela última vez.
   - **Ao acessar e modificar**

     O Kaspersky Embedded Systems Security 2.2 verifica o objeto quando for aberto e novamente após ser salvo, caso tenha sido modificado.

     Esta opção é selecionada por padrão.
   - **Ao acessar**

     O Kaspersky Embedded Systems Security 2.2 verifica todos os objetos quando eles são abertos para leitura ou para execução ou modificação.
   - **Ao executar**

     O Kaspersky Embedded Systems Security 2.2 verificará o arquivo apenas quando ele for acessado para ser executado.
5. Clique em **OK**.

O modo de proteção selecionado entrará em vigor.

Escopo da proteção na tarefa de Proteção de Arquivos em Tempo Real

Esta seção fornece instruções sobre a criação e o gerenciamento de um escopo da proteção na tarefa de Proteção de Arquivos em Tempo Real.

Nesta seção

Escopos da proteção predefinidos

Os recursos de arquivo do computador protegido são exibidos nas configurações da tarefa **Proteção de Arquivos em Tempo Real** na guia **Escopo da proteção**.

A árvore ou a lista de recursos de arquivos exibem os nós aos quais você tem o acesso à leitura com base nas configurações de segurança definidas do Microsoft Windows.

O Kaspersky Embedded Systems Security 2.2 abrange os seguintes escopos da proteção predefinidos:

- **Discos rígidos locais**. O Kaspersky Embedded Systems Security 2.2 protege arquivos nos discos rígidos de computador.
- **Unidades removíveis**. O Kaspersky Embedded Systems Security 2.2 protege arquivos em dispositivos externos, como unidades USB ou em CDs. É possível incluir ou excluir do escopo da proteção todos os discos removíveis, discos, pastas ou arquivos individuais.
- **Rede**. O Kaspersky Embedded Systems Security 2.2 verifica os arquivos gravados em pastas de redes ou lidos nelas por aplicativos em execução no computador. O Kaspersky Embedded Systems Security 2.2 não protege os arquivos quando eles são acessados por aplicativos de outros computadores.
- **Unidades virtuais**. Pastas e arquivos dinâmicos, e unidades que são temporariamente conectadas ao computador podem ser incluídos no escopo da proteção, por exemplo, unidades de cluster comuns.

Por padrão, você pode visualizar e configurar escopos da proteção predefinidos na lista de escopo; você também pode adicionar escopos predefinidos à lista durante sua formação nas configurações do escopo da proteção.

Por padrão, o escopo da proteção inclui todas as áreas predefinidas, exceto unidades virtuais.

As unidades virtuais criadas usando o comando SUBST não são exibidas na árvore de recursos de arquivos do computador no Console do Aplicativo. Para incluir objetos da unidade virtual no escopo da proteção, inclua a pasta do computador à qual essa unidade virtual está associada no escopo da proteção.
As unidades de rede conectadas também não serão exibidas na lista de recursos de arquivos do computador. Para incluir objetos das unidades de rede no escopo da proteção, especifique o caminho da pasta que corresponde a essa unidade de rede no formato UNC.

Seleção de níveis de segurança predefinidos

Um dos seguintes níveis de segurança predefinidos para os nós selecionados na lista de recursos do arquivo do computador pode ser aplicado: **Desempenho máximo**, **Recomendado** e **Proteção máxima**. Cada um desses níveis contém seu próprio conjunto de configurações de segurança predefinido (veja a tabela abaixo).

Desempenho máximo

O nível de segurança **Desempenho máximo** é recomendado se, além de usar o Kaspersky Embedded Systems Security 2.2 nos computadores, existirem medidas de segurança adicionais nos computadores dentro da rede, por exemplo, Firewalls e políticas de segurança existentes.

Recomendado

O nível de segurança **Recomendado** assegura uma combinação ideal de impacto de proteção e desempenho nos computadores protegidos. Esse nível é recomendado pelos especialistas da Kaspersky Lab como suficiente para proteger computadores na maioria das redes corporativas. O nível de segurança **Recomendado** é configurado por padrão.

Proteção máxima

O nível de segurança de **Proteção máxima** é recomendado se a rede da sua organização tiver requisitos elevados de segurança para seus computadores.

Tabela 31. Níveis de segurança predefinidos e valores de configurações correspondentes

Opções	Nível de segurança		
	Desempenho máximo	Recomendado	Proteção máxima
Proteção de objetos	Por extensão	Por formato	Por formato
Proteger somente arquivos novos e modificados	Ativado	Ativado	Desativado
Ação a ser executada em objetos infectados e outros	Bloquear acesso e desinfectar. Remover se a desinfecção falhar	Bloquear acesso e executar ação recomendada	Bloquear acesso e desinfectar. Remover se a desinfecção falhar
Ação a ser executada em objetos possivelmente infectados	Bloquear acesso e colocar na quarentena	Bloquear acesso e executar ação recomendada	Bloquear acesso e colocar na quarentena
Excluir arquivos	Não	Não	Não
Não detectar	Não	Não	Não
Parar a verificação se demorar mais que (s)	60 seg.	60 seg.	60 seg.
Não verificar objetos compostos com mais de (MB)	8 MB	8 MB	Não definido
Verificar fluxos NTFS alternativos	Sim	Sim	Sim
Verificar setores de inicialização do disco e MBR	Sim	Sim	Sim

Opções	Nível de segurança		
Proteção de objetos compostos	• Objetos compactados* *Somente objetos novos e modificados	• Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* *Somente objetos novos e modificados	• Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* *Todos os objetos
Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte objeto incorporado	Não	Não	Sim

As configurações **Proteção de objetos**, **Usar a tecnologia iChecker**, **Usar a tecnologia iSwift** e **Usar o analisador heurístico** não estão incluídas nas configurações dos níveis de segurança predefinidos. Se você editar as configurações de segurança **Proteção de objetos**, **Usar a tecnologia iChecker**, **Usar a tecnologia iSwift** ou **Usar o analisador heurístico** após selecionar um dos níveis de segurança predefinidos, o nível de segurança que selecionou não será alterado.

► *Para selecionar um dos níveis de segurança predefinidos, execute as seguintes etapas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Proteção do Computador em Tempo Real** clique no botão **Configurações** no bloco **Proteção de arquivos em tempo real**.

   A janela **Proteção de arquivos em tempo real** é aberta.
4. Na guia **Escopo da proteção**, selecione o nó cujas configurações de segurança você deseja definir e clique em **Configurar**.

   A janela **Configurações de Proteção de arquivos em tempo real** é aberta.

5. Selecione o nível de segurança desejado na lista suspensa:
   - **Proteção máxima**
   - **Recomendado**
   - **Desempenho máximo**
6. Clique em **OK**.

As configurações recém-definidas foram salvas.

O Kaspersky Embedded Systems 2.2 aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora quando as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de tarefas.

Definição manual de configurações de segurança

Por padrão, a tarefa de Proteção de Arquivos em Tempo Real usa as configurações de segurança comuns para todo o escopo da proteção. Estas configurações correspondem ao nível de segurança predefinido **Recomendado** (consulte a seção "Seleção de níveis de segurança predefinidos" na página 153).

Os valores padrão das configurações de segurança podem ser modificados, definindo-os como configurações comuns para todo o escopo da proteção ou como configurações diferentes para nós diferentes da árvore de recursos ou lista de arquivos do computador.

Ao trabalhar com a árvore de recursos de arquivo de computador, as configurações de segurança definidas para o nó pai selecionado são automaticamente aplicadas a todos os nós filhos. As configurações de segurança do nó pai não são aplicadas a nós filhos configurados separadamente.

► *Para definir as configurações de segurança do nó selecionado manualmente:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Proteção do Computador em Tempo Real** clique no botão **Configurações** no bloco **Proteção de arquivos em tempo real**.

   A janela **Proteção de arquivos em tempo real** é aberta.

4. Na guia **Escopo da proteção**, selecione o nó cujas configurações de segurança você deseja definir e clique em **Configurar**.

   A janela **Configurações de Proteção de arquivos em tempo real** é aberta.

5. Na guia **Nível de segurança** você pode selecionar qualquer nível existente ou clicar no botão **Configurações** para definir uma configuração personalizada.

6. É possível definir configurações de segurança personalizadas do nó selecionado, de acordo com os seus requisitos:

   - As configurações gerais (consulte a seção "Definir configurações gerais de tarefas" na página 156)
   - Ações (consulte a seção "Configurar ações" na página 158)
   - Desempenho (consulte a seção "Configurar o desempenho" na página 160)

7. Clique em **Salvar** na janela **Configurações do escopo da proteção**.

As novas configurações de escopo da proteção são salvas.

Definir configurações gerais de tarefas

► *Para definir as configurações gerais da tarefa de Proteção de Arquivos em Tempo Real:*

1. Abra a janela **Configurações de Proteção de arquivos em tempo real** (consulte a seção "Definição manual de configurações de segurança" na página 155).

2. Selecione a guia **Geral**.

3. Na seção **Proteção de objetos**, especifique os tipos de objetos que deseja incluir no escopo da proteção:

   - **Todos os objetos**

     O Kaspersky Embedded Systems Security 2.2 verifica todos os objetos.

   - **Objetos verificados por formato**

     O Kaspersky Embedded Systems Security 2.2 verificará somente objetos infectáveis com base no formato do arquivo.

     A lista de formatos é compilada pela Kaspersky Lab. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security 2.2.

   - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados de antivírus**

     O Kaspersky Embedded Systems Security 2.2 verificará somente objetos infectáveis com base na extensão do arquivo.

     A lista de extensões é compilada pela Kaspersky Lab. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security 2.2.

   - **Objetos verificados pela lista de extensões especificada**

     O Kaspersky Embedded Systems Security 2.2 verificará os arquivos baseados em suas extensões. A lista de extensões de arquivo pode ser personalizada manualmente na janela **Lista de extensões**, que pode ser exibida clicando no botão **Editar**.

- **Verificar setores de inicialização do disco e MBR**

  Ativa a proteção dos setores de inicialização e dos registros mestres de inicialização.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 verificará os setores de inicialização e os registros mestres de inicialização nos discos rígidos e unidades removíveis do computador.

  A caixa de seleção é selecionada por padrão.

- **Verificar fluxos NTFS alternativos**

  Verificação de fluxos alternativos de arquivos e pastas nas unidades do sistema de arquivos NTFS.

  Se a caixa estiver selecionada, o aplicativo verifica um objeto possivelmente infectado e todos os fluxos NTFS associados àquele objeto.

  Se a caixa estiver desmarcada, o aplicativo verifica apenas o objeto detectado e considerado possivelmente infectado.

  A caixa de seleção é selecionada por padrão.

4. Na seção **Desempenho**, selecione ou desmarque a caixa **Proteger somente arquivos novos e modificados**.

   Esta caixa ativa/desativa a verificação e a proteção de arquivos que foram reconhecidas pelo Kaspersky Embedded Systems Security 2.2 como novos ou modificados desde a última verificação.

   Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 verificará e protegerá apenas os arquivos reconhecidos como novos ou modificados desde a última verificação.

   Se a caixa estiver desmarcada, você poderá selecioná-la se quiser verificar e proteger apenas arquivos novos ou todos os arquivos, desconsiderando o status de modificação.

   Por padrão, a caixa de seleção é selecionada para os níveis de segurança de **Desempenho máximo** e **Recomendado**. Se o nível de segurança **Proteção máxima** estiver definido, a caixa será desmarcada.

> Para alternar entre as opções disponíveis quando a caixa estiver desmarcada, clique no link **Todos / Apenas novos** para cada um dos tipos de objetos compostos.

5. Na seção **Proteção de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da proteção:

- **Todos / Apenas arquivos compactados novos**

  Verificação dos arquivos comprimidos ZIP, CAB, RAR, ARJ e de outros formatos.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 verificará os arquivos compactados.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 ignorará os arquivos compactados durante a verificação.

  O valor padrão depende do nível de segurança selecionado.

- **Todos/Apenas arquivos compactados SFX novos**

  Verificação de arquivos compactados autoextraíveis.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2

verificará os arquivos compactados SFX.

Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 ignorará os arquivos compactados SFX durante a verificação.

O valor padrão depende do nível de segurança selecionado.

Esta opção fica ativa quando a caixa de seleção **Arquivos compactados** é desmarcada.

- **Todos/Apenas novos bancos de dados de e-mail**

  Verificação de arquivos de banco de dados de correio do Microsoft Outlook® e Microsoft Outlook Express.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 verificará os arquivos de bancos de dados de correio.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 ignorará os arquivos de bancos de dados de correio durante a verificação.

  O valor padrão depende do nível de segurança selecionado.

- **Todos / Apenas objetos compactados novos**

  Verificação de arquivos executáveis compactados por compactadores de código binário, como UPX ou ASPack.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 verificará os arquivos executáveis compactados por compactadores de código binário.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 ignorará os arquivos executáveis compactados por compactadores de código binário durante a verificação.

  O valor padrão depende do nível de segurança selecionado.

- **Todos / Apenas e-mails sem formatação novos**

  Verificação de arquivos de formato de e-mail, como mensagens do Microsoft Outlook e Microsoft Outlook Express.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 verificará os arquivos de formato de e-mail.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 ignorará os arquivos de formato de e-mail durante a verificação.

  O valor padrão depende do nível de segurança selecionado.

- **Todos / Apenas objetos OLE incorporados novos**

  Verificação de objetos incorporados em arquivos (como macros do Microsoft Word ou anexos de e-mail).

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 verificará os objetos incorporados a arquivos.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 ignorará os objetos incorporados a arquivos durante a verificação.

  O valor padrão depende do nível de segurança selecionado.

6. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Configurar ações

► *Para configurar as ações em objetos infectados e outros objetos detectados da tarefa Proteção de Arquivos em Tempo Real:*

1. Abra a janela **Configurações de Proteção de arquivos em tempo real** (consulte a seção "Definição manual de configurações de segurança" na página 155).
2. Selecione a guia **Ações**.
3. Selecione a ação a ser executada em objetos infectados e outros objetos detectados.
   - **Somente notificações**.

     Quando este modo for selecionado, o Kaspersky Embedded Systems Security 2.2 não bloqueia o acesso a objetos infectados ou outros objetos detectados, ou executa qualquer ação neles. O seguinte evento é registrado no log de tarefas: *Objeto não desinfectado. Motivo: nenhuma ação foi executada para neutralizar o objeto detectado devido a configurações definidas pelos usuários.* O evento especifica todas as informações disponíveis sobre o objeto detectado.

     O modo **Somente notificações** deve ser configurado separadamente para cada área de proteção. Este modo não é usado por padrão para qualquer um dos níveis de segurança. Se este modo for selecionado, o Kaspersky Embedded Systems Security 2.2 altera automaticamente o nível de segurança **Personalizado**.
   - **Bloquear acesso**.

     Quando esta opção é selecionada o Kaspersky Embedded Systems Security 2.2 bloqueia o acesso ao objeto detectado ou possivelmente infectado. É possível selecionar ação adicional para objetos bloqueados na lista suspensa.
   - **Executar ação adicional**.

     Selecionar ação da lista suspensa:
     - **Desinfectar**.
     - **Desinfectar. Remover se a desinfecção falhar**.
     - **Remover**.
     - **Recomendado**.
4. Selecione a ação a ser executada em objetos possivelmente infectados:
   - **Somente notificações**.

     Quando este modo for selecionado, o Kaspersky Embedded Systems Security 2.2 não bloqueia o acesso a objetos infectados ou outros objetos detectados, ou executa qualquer ação neles. O seguinte evento é registrado no log de tarefas: *Objeto não desinfectado. Motivo: nenhuma ação foi executada para neutralizar o objeto detectado devido a configurações definidas pelos usuários.* O evento especifica todas as informações disponíveis sobre o objeto detectado.

     O modo **Somente notificações** deve ser configurado separadamente para cada área de proteção. Este modo não é usado por padrão para qualquer um dos níveis de segurança. Se este modo for selecionado, o Kaspersky Embedded Systems Security 2.2 altera automaticamente o nível de segurança **Personalizado**.
   - **Bloquear acesso**.

     Quando esta opção é selecionada o Kaspersky Embedded Systems Security 2.2 bloqueia o acesso ao objeto detectado ou possivelmente infectado. É possível selecionar ação adicional para objetos bloqueados na lista suspensa.

- **Executar ação adicional**.

  Selecionar ação da lista suspensa:

  - **Quarentena**.
  - **Remover**.
  - **Recomendado**.

5. Configure ações a ser executadas em objetos dependendo do tipo de objeto detectado:

   a. Desmarque ou selecione a caixa **Executar ações dependendo do tipo de objeto detectado**.

   Se a caixa for selecionada, você pode definir a ação primária e secundária para cada tipo de objeto detectado clicando no botão **Configurações** ao lado da caixa.

   Se a caixa for desmarcada, o Kaspersky Embedded Systems Security 2.2 executa as ações selecionadas nas seções **Ação a ser executada em objetos infectados e outros** e **Ação a ser executada em objetos possivelmente infectados** para os tipos de objetos indicados, respectivamente.

   Esta caixa é desmarcada por padrão.

   b. Clique no botão **Configurações**.

   c. Na janela que se abre, selecione a ação primária e secundária (se a primeira ação falhar) para cada tipo do objeto detectado.

   d. Clique em **OK**.

6. Selecione a ação a ser executada em arquivos compostos não modificáveis: selecione ou desmarque a caixa **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte objeto incorporado**.

   Esta caixa ativa ou desativa a remoção forçada do arquivo composto pai quando um objeto malicioso, possivelmente infectado ou outro objeto filho incorporado for detectado.

   Se a caixa estiver selecionada e a tarefa for configurada para remover objetos infectados e possivelmente infectados, o Kaspersky Embedded Systems Security 2.2 forçosamente remove o objeto composto pai quando um objeto incorporado malicioso ou outro for detectado. A remoção forçada de um arquivo pai juntamente com todo o seu conteúdo ocorre se o aplicativo não puder remover apenas o objeto filho detectado (por exemplo, se o objeto pai não pode ser modificado).

   Se esta caixa estiver desmarcada e a tarefa for configurada para objetos infectado e possivelmente infectados, o Kaspersky Embedded Systems Security 2.2 não executa a ação selecionada se o objeto pai não puder ser modificado.

   Por padrão, a caixa é selecionada para o nível de segurança de **Proteção máxima** e desmarcada para os níveis de segurança **Recomendado** e **Desempenho máximo**.

7. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Configurar o desempenho

► *Para configurar o desempenho da tarefa de Proteção de Arquivos em Tempo Real:*

1. Abra a janela **Configurações de Proteção de arquivos em tempo real** (consulte a seção "Definição manual de configurações de segurança" na página 155).
2. Selecione a guia **Desempenho**.
3. Na seção **Exclusões**:
   - Desmarque ou selecione a caixa **Excluir arquivos**.

     Excluindo arquivos da verificação pelo nome de arquivo ou pela máscara de nome de arquivo.

     Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 ignorará os objetos especificados durante a verificação.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 verificará todos os objetos.

     Esta caixa é desmarcada por padrão.
   - Desmarque ou selecione a caixa **Não detectar**.

     Os objetos são excluídos da verificação por meio do nome ou da máscara de nome do objeto detectável. A lista de nomes de objetos detectáveis está disponível no site da Enciclopédia de Vírus http://www.securelist.com.

     Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 ignorará os objetos detectáveis especificados durante a verificação.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 detectará todos os objetos especificados no aplicativo por padrão.

     Esta caixa é desmarcada por padrão.
   - Clique no botão **Editar** de cada configuração para adicionar exclusões.
4. Na seção **Configurações avançadas**:
   - **Parar a verificação se demorar mais que (s)**

     Limita a duração da verificação do objeto. O valor padrão é 60 segundos.

     Se a caixa de seleção estiver selecionada, a duração da verificação será limitada ao valor especificado.

     Se a caixa de seleção estiver desmarcada, a duração da verificação será ilimitada.

     A caixa de seleção é selecionada por padrão.
   - **Não verificar objetos compostos com mais de (MB)**

     Exclui objetos maiores do que o tamanho especificado na verificação.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 ignorará objetos compostos cujo tamanho exceda o limite especificado durante a verificação de vírus.

     Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 verificará os objetos compostos de qualquer tamanho.

     Por padrão, a caixa de seleção está selecionada para os níveis de segurança **Recomendado** e **Desempenho máximo**.

- **Usar a tecnologia iSwift**

  A tecnologia iSwift compara o identificador NTFS do arquivo armazenado em um banco de dados com um identificador atual. A verificação é executada apenas para arquivos cujos identificadores foram alterados (novos arquivos e arquivos modificados desde a última verificação dos objetos do sistema NTFS).

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 verificará apenas os novos arquivos ou aqueles modificados desde a última verificação dos objetos do sistema NTFS.

  Se a caixa de verificação estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 verificará os arquivos do sistema NTFS sem considerar a data de criação ou modificação.

  A caixa de seleção é selecionada por padrão.

- **Usar a tecnologia iChecker**

  A tecnologia iChecker calcula e lembra de somas de verificação de arquivos verificados. Se um objeto for modificado a soma de verificação é alterada. O aplicativo compara todas as somas de verificação durante a tarefa de verificação e verifica apenas objetos novos e modificados desde a última verificação de arquivos.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security 2.2 verificará apenas arquivos novos e modificados.

  Se a caixa de verificação estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 verificará os arquivos sem considerar a data de criação ou modificação.

  A caixa de seleção é selecionada por padrão.

5. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Uso da KSN

Esta seção contém informações sobre a tarefa de Uso da KSN e como configurá-la.

Nesta seção

Sobre a tarefa de Uso da KSN

A *Kaspersky Security Network* (também referida como “KSN”) é uma infraestrutura de serviços on-line que fornece acesso à base de conhecimentos operacionais da Kaspersky Lab sobre a reputação de arquivos, de recursos da web e de programas. A Kaspersky Security Network permite ao Kaspersky Embedded Systems Security 2.2

reagir muito rapidamente a novas ameaças, melhora o desempenho de vários componentes de proteção e reduz a probabilidade de falsos positivos.

Para iniciar a tarefa de Uso da KSN, você deve aceitar a Declaração da Kaspersky Security Network.

As informações recebidas pelo Kaspersky Embedded Systems Security 2.2 da Kaspersky Security Network referem-se apenas à reputação de programas.

A participação na KSN permite que a Kaspersky Lab receba informações em tempo real sobre os tipos e fontes de novas ameaças, desenvolva modos de neutralizá-las e reduza o número de falsos positivos em componentes de aplicativo.

Mais informações detalhadas sobre a transferência, o processamento, armazenamento e a destruição de informações sobre o uso do aplicativo está disponível na janela Manuseio de dados da tarefa de Uso da KSN e na Política de Privacidade no site da Kaspersky Lab.

A participação na Kaspersky Security Network é voluntária. A decisão quanto à participação na Kaspersky Security Network é tomada durante ou após a instalação do Kaspersky Embedded Systems Security 2.2. É possível modificar a sua decisão sobre a participação na Kaspersky Security Network a qualquer momento.

A Kaspersky Security Network pode ser usada nas seguintes tarefas do Kaspersky Embedded Systems Security 2.2:

- Proteção de Arquivos em Tempo Real.
- Verificação por Demanda.
- Controle de Inicialização de Aplicativos.

Kaspersky Private Security Network

Veja detalhes sobre como configurar a Kaspersky Private Security Network (também referida como “KSN Particular”) no *Kaspersky Security Center*.

Se você usar a KSN Particular no computador protegido, na janela **Manuseio de dados** (consulte a seção "Configurando o processamento de dados" na página 167) da tarefa de Uso da KSN, é possível ler a Declaração da KSN e ativar a tarefa selecionando **Eu aceito os termos da Declaração da Kaspersky Private Security Network**. Ao aceitar os termos, você aceita enviar todos os tipos de dados mencionados na Declaração da KSN (solicitações de segurança, dados estatísticos) aos serviços da KSN.

Depois de aceitar os termos da KSN Particular, as caixas que ajustam o uso da KSN Global não estarão disponíveis.

Se você desativar a KSN Particular quando a tarefa de Uso da KSN estiver em execução, o erro *Violação da licença* ocorrerá e a tarefa será interrompida. Para continuar protegendo o computador, será necessário aceitar a Declaração da KSN na janela **Manuseio de dados** e reiniciar a tarefa.

Cancelar a aceitação da Declaração da KSN

Você pode cancelar a aceitação e interromper qualquer troca de dados com a Kaspersky Security Network a qualquer momento. As seguintes ações são consideradas como o cancelamento total ou parcial da Declaração da KSN:

- Desmarcar a caixa **Enviar dados dos arquivos verificados**: o aplicativo deixa de enviar somas de verificação de arquivos verificados ao serviço KSN para análise.
- Desmarcar a caixa **Enviar as estatísticas da Kaspersky Security Network**: o aplicativo deixa de processar dados com estatísticas adicionais da KSN.
- Desmarcar a caixa **Eu aceito os termos da Declaração da Kaspersky Security Network**: o aplicativo interrompe todo o processamento de dados relacionado à KSN e também interrompe a tarefa de Uso da KSN.
- Desinstalar o componente Uso da KSN: todo processamento de dados relacionado à KSN é interrompido.
- Desinstalar o Kaspersky Embedded Systems Security 2.2: todo processamento de dados relacionado à KSN é interrompido.

Configurando a tarefa de Uso da KSN

É possível alterar as configurações padrão da tarefa de Uso da KSN (consulte a tabela abaixo).

Tabela 32. Configurações padrão da tarefa de Uso da KSN

Configuração	Valor padrão	Descrição
Ações a serem executadas em objetos não confiáveis da KSN	Remover	Você pode especificar ações que o Kaspersky Embedded Systems Security 2.2 executará em objetos identificados pela KSN como não confiáveis.
Transferência de dados	A soma de verificação de arquivo (hash MD5) é calculada para arquivos que não excedam 2 MB de tamanho.	Você pode especificar o tamanho máximo de arquivos para os quais uma soma de verificação é calculada usando o algoritmo MD5 para a entrega à KSN. Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 calculará o hash MD5 para arquivos de qualquer tamanho.
Declaração da KSN	A caixa **Eu aceito os termos da Declaração da Kaspersky Security Network** é desmarcada.	Decida se quer participar na KSN após a instalação. Você pode alterar a sua decisão a qualquer momento.
Enviar as estatísticas da Kaspersky Security Network	Selecionado (aplica-se apenas se a Declaração da KSN for aceita)	Se a Declaração da KSN for aceita, as estatísticas da KSN serão enviadas automaticamente, a menos que você desmarque a caixa.
Enviar dados dos arquivos verificados	Selecionado (aplica-se apenas se a Declaração da KSN for aceita)	Se a Declaração do KSN for aceita, os dados dos arquivos verificados e analisados desde que a tarefa foi iniciada são enviados. Você pode desmarcar a caixa a qualquer momento.
Aceito os termos da Declaração da Kaspersky Managed Protection	Desmarcado	Você pode ativar ou desativar o serviço KMP. O serviço fica disponível apenas se o acordo adicional tiver sido assinado durante o processo de compra do aplicativo.

Configuração	Valor padrão	Descrição
Programação de inicialização de tarefa	A primeira execução não está programada.	É possível iniciar a tarefa manualmente ou configurar um início programado.
Usar o Kaspersky Security Center como Proxy da KSN	Selecionado	Por padrão, os dados são enviados à KSN por meio do Kaspersky Security Center.

► *Para configurar a tarefa de Uso da KSN, siga as etapas a seguir:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Proteção do Computador em Tempo Real**, clique no botão **Configurações** no bloco **Uso da KSN**.

   A janela **Uso da KSN** é exibida.
4. Na guia **Geral**, defina as seguintes configurações de tarefa:
   - Na seção **Ação a ser executada nos objetos não confiáveis da KSN**, especifique a ação que o Kaspersky Embedded Systems Security 2.2 deverá executar se detectar um objeto identificado pela KSN como infectado:
     - **Remover**

       O Kaspersky Embedded Systems Security 2.2 exclui o objeto com o status não confiável da KSN e coloca uma cópia dele no Backup.

       Esta opção é selecionada por padrão.
     - **Informações de log**

       O Kaspersky Embedded Systems Security 2.2 registra informações sobre o objeto com o status não confiável da KSN no log de tarefas. O Kaspersky Embedded Systems Security 2.2 não exclui o objeto não confiável.

- Na seção **Transferência de dados**, restrinja o tamanho dos arquivos para que a soma de verificação seja calculada:
  - Desmarque ou selecione a caixa **Não calcular a soma de verificação antes de enviar à KSN se o tamanho do arquivo ultrapassar (MB)**.

    Esta caixa ativa ou desativa o cálculo da soma de verificação para arquivos do tamanho especificado para a entrega destas informações ao serviço da KSN.

    A duração do cálculo de soma de verificação depende do tamanho do arquivo.

    Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security 2.2 não calculará a soma de verificação de arquivos que excedam o tamanho especificado (em MB).

    Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 calculará a soma de verificação para arquivos de qualquer tamanho.

    A caixa de seleção é selecionada por padrão.
  - Se necessário, no campo à direita, especifique o tamanho máximo de arquivos para os quais o Kaspersky Embedded Systems Security 2.2 calcula a soma de verificação.
- Desmarque ou selecione a caixa **Usar o Kaspersky Security Center como Proxy da KSN**.

  A caixa permite gerenciar a transferência de dados entre os computadores protegidos e a KSN.

  Se a caixa for desmarcada os dados do Servidor de Administração e dos computadores protegidos são enviados à KSN diretamente (não via o Kaspersky Security Center). A política ativa define que tipo de dados pode ser enviado à KSN diretamente.

  Se a caixa for selecionada, todos os dados são enviados à KSN via o Kaspersky Security Center.

  A caixa de seleção é selecionada por padrão.

> Para ativar o Proxy da KSN a Declaração da KSN deve ser aceita e o Kaspersky Security Center propriamente configurado. Consulte a *Ajuda do Kaspersky Security Center* para mais detalhes.

5. Se necessário, configure a programação de início da tarefa na guia **Gerenciamento de tarefa**. Por exemplo, você pode ativar o início da tarefa por programação e especificar a frequência de início da tarefa **Ao iniciar o aplicativo** se desejar que a tarefa seja executada automaticamente quando o computador for reiniciado.

   O aplicativo iniciará automaticamente a tarefa de Uso da KSN de acordo com a programação.
6. Configure o manuseio de dados (consulte a seção "Configurando o processamento de dados" na página 167) antes de iniciar a tarefa.
7. Clique em **OK**.

As configurações modificadas são aplicadas. A data e hora da modificação das configurações, bem como informações sobre as configurações de tarefa antes e após a modificação, são salvas no log de tarefas.

Configurando o processamento de dados

► *Para configurar quais dados serão processados pelos serviços da KSN e aceitar a Declaração da KSN:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

     Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Proteção do Computador em Tempo Real** clique no botão **Manuseio de dados** no bloco **Uso da KSN**.

   A janela **Manuseio de dados** é exibida.
4. Na guia **Estatísticas e serviços**, leia a Declaração e selecione a caixa **Eu aceito os termos da Declaração da Kaspersky Security Network**.
5. Para aumentar o nível de proteção, as seguintes caixas são selecionadas automaticamente:
   - **Enviar dados dos arquivos verificados**.

     Se a caixa for selecionada, o Kaspersky Embedded Systems Security 2.2 envia a soma de verificação dos arquivos verificados para a Kaspersky Lab. A conclusão sobre a segurança de cada arquivo baseia-se na reputação recebida da KSN.

     Se a caixa for desmarcada, o Kaspersky Embedded Systems Security 2.2 não envia a soma de verificação dos arquivos à KSN.

     Note que as solicitações de reputação de arquivos poderiam ser enviadas em um modo limitado. As limitações são usadas para proteger os servidores de reputação da Kaspersky Lab de ataques DDoS. Neste cenário, os parâmetros das solicitações de reputação de arquivos sendo enviados são definidos pelas regras e pelos métodos estabelecidos por especialistas da Kaspersky Lab, e não podem ser configurados pelo usuário em um computador protegido. As atualizações dessas regras e métodos são recebidas juntamente com as atualizações do banco de dados do aplicativo. Se as limitações forem aplicadas, o status *Ativado pela Kaspersky Lab para proteger os servidores KSN contra DDoS* é exibido na estatística da tarefa de Uso da KSN.

     A caixa de seleção é selecionada por padrão.
   - **Enviar as estatísticas da Kaspersky Security Network.**

     Se a caixa for selecionada o Kaspersky Embedded Systems Security 2.2 envia estatísticas adicionais que podem conter dados pessoais. A lista de todos os dados enviados como estatística da KSN é especificada na Declaração da KSN. Os dados recebidos pela Kaspersky Lab são usados para melhorar a qualidade dos aplicativos e as taxas de detecção de ameaças.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 não enviará estatísticas adicionais. A caixa de seleção é selecionada por padrão.

Você pode desmarcar estas caixas e deixar de enviar dados adicionais a qualquer momento.

6. Na guia **Kaspersky Managed Protection**, leia a Declaração e selecione a caixa **Eu aceito os termos da Kaspersky Managed Protection**.

   Se a caixa for selecionada, você aceita enviar estatísticas das atividades do computador protegido aos especialistas da Kaspersky Lab. Os dados recebidos serão usados para análise e reporte contínuos, necessários para impedir incidentes de violação de segurança.

   Esta caixa é desmarcada por padrão.

   Alterações no status da caixa **Eu aceito os termos da Kaspersky Managed Protection** não iniciam ou interrompem o processamento de dados imediatamente. Para aplicar as alterações, é necessário reiniciar o Kaspersky Embedded Systems Security 2.2.

   Para usar o serviço KMP, é necessário assinar o acordo correspondente e executar os arquivos de configuração em um computador protegido.

   Para usar o serviço KMP os termos de processamento de dados da Declaração da KSN na guia **Estatísticas e serviços** devem ser aceitos.

7. Clique em **OK**.

   A configuração de processamento de dados será salva.

Configurando a transferência de dados adicionais

O Kaspersky Embedded Systems Security 2.2 pode ser configurado para enviar os seguintes dados à Kaspersky Lab:

- Somas de verificação de arquivos verificados (caixa de seleção **Enviar dados dos arquivos verificados**).
- Estatísticas adicionais, inclusive dados pessoais (caixa de seleção **Enviar as estatísticas da Kaspersky Security Network**).

Consulta a seção "Tratamento local de dados" neste manual para obter informações detalhadas sobre dados enviados à Kaspersky Lab.

As caixas correspondentes podem ser selecionadas ou desmarcadas apenas se a caixa **Eu aceito os termos da Declaração da Kaspersky Security Network** estiver selecionada.

Por padrão, o Kaspersky Embedded Systems Security 2.2 envia somas de verificação de arquivos e estatísticas adicionais após aceitar a Declaração da KSN.

Tabela 33. Estados possíveis de caixas de seleção e condições correspondentes

Estado da caixa	Condições de estado da caixa **Enviar dados dos arquivos verificados**	Condições de estado da caixa **Enviar as estatísticas da Kaspersky Security Network**
☑	• solicitações de reputação são enviadas • a caixa pode ser editada	• estatísticas adicionais são enviadas • a caixa pode ser editada
☑ (inativa)	• solicitações de reputação não são enviadas • a caixa não pode ser editada	• estatísticas adicionais não são enviadas • a caixa não pode ser editada
☐	• solicitações de reputação não são enviadas • a caixa pode ser editada	• estatísticas adicionais não são enviadas • a caixa pode ser editada
☐ (inativa)	• solicitações de reputação não são enviadas • a caixa não pode ser editada	• estatísticas adicionais não são enviadas • a caixa não pode ser editada

Prevenção de Exploits

Esta seção contém instruções sobre como definir configurações de proteção da memória do processo.

Neste capítulo

Sobre a Prevenção de Exploits

O Kaspersky Embedded Systems Security 2.2 oferece a capacidade de proteger a memória do processo contra exploits. Este recurso é implementado no componente de Prevenção de Exploits. Você pode alterar o status da atividade do componente e definir configurações de proteção da memória do processo.

O componente protege a memória do processo contra exploits inserindo um Agente de Proteção de Processo ("Agente") externo no processo protegido.

Um Agente de Proteção de Processo é um módulo do Kaspersky Embedded Systems Security 2.2, dinamicamente carregado, inserido em processos protegidos para monitorar a sua integridade e reduzir o risco de eles serem explorados.

A operação do Agente dentro do processo protegido exige a inicialização e a interrupção do processo: o carregamento inicial do Agente em um processo acrescentado à lista de processos protegidos só é possível se o processo for reiniciado. Além disso, depois que um processo foi removido da lista de processos protegidos, o Agente poderá ser descarregado somente depois que o processo foi reiniciado.

O Agente deve ser interrompido para descarregá-lo dos processos protegidos: se o componente de Prevenção de Exploits for desinstalado, o aplicativo congelará o ambiente e forçará o Agente a ser descarregado dos processos protegidos. Se durante a desinstalação do componente o Agente for introduzido em algum dos processos protegidos, você deverá terminar o processo afetado. O reinício do computador pode ser necessário (por exemplo, se o processo do sistema estiver sendo protegido).

Se for detectada evidência de um ataque de exploit em um processo protegido, o Kaspersky Embedded Systems Security 2.2 executará uma das seguintes ações:

- Encerrará o processo se uma tentativa de exploit for feita.
- Informará que o processo foi comprometido.

É possível interromper a proteção do processo usando um dos seguintes métodos:

- Desinstalação do componente.
- Remoção do processo da lista de processos protegidos e a sua reinicialização.

Kaspersky Security Exploit Prevention Service

O Kaspersky Security Exploit Prevention Service é necessário no computador protegido para que o componente de Prevenção de Exploits seja eficaz. Este serviço e o componente de Prevenção de Exploits fazem parte da instalação recomendada. Durante a instalação do serviço no computador protegido, o processo kavfswh é criado e iniciado. Ele comunica as informações sobre processos protegidos do componente para o Agente de Segurança.

Depois que o Kaspersky Security Exploit Prevention Service for interrompido, o Kaspersky Embedded Systems Security 2.2 continua a proteger os processos adicionados à lista de processos protegidos, também é carregado nos processos recém-adicionados e aplica todas as técnicas disponíveis de prevenção de exploits para proteger a memória do processo.

Se o Kaspersky Security Exploit Prevention Service for interrompido, o aplicativo não receberá informações sobre os eventos que ocorrem com os processos protegidos (inclusive informações sobre ataques de exploits e o encerramento de processos). Além disso, o Agente não será capaz de receber informações sobre novas configurações de proteção e a adição de novos processos à lista de processos protegidos.

Modo de Prevenção de Exploits

É possível selecionar um dos seguintes modos para configurar ações para reduzir os riscos de que vulnerabilidades sejam exploradas em processos protegidos:

- **Encerrar no exploit**: aplique este modo para encerrar um processo quando uma tentativa de exploit for feita.

  Após detecção de uma tentativa de explorar uma vulnerabilidade em um processo crítico do sistema operacional protegido, o Kaspersky Embedded Systems Security 2.2 encerrará o processo, independentemente do modo indicado nas configurações do componente de Prevenção de Exploits.

- **Somente notificar processos violados**: aplique este modo para receber informações sobre exemplos de exploits em processos protegidos usando eventos na Auditoria de Segurança Filtrada.

  Se este modo for selecionado, o Kaspersky Embedded Systems Security 2.2 registra em log todas as tentativas de explorar vulnerabilidades durante a criação de eventos.

Definição das configurações de proteção da memória do processo

► *Para definir configurações para proteger a memória de processos adicionados à lista de processos protegidos, realize as seguintes ações:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
    - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
    - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

    > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Proteção do Computador em Tempo Real** clique no botão **Configurações** no bloco **Prevenção de Exploits**.

    A janela **Prevenção de Exploits** é exibida.
4. Na seção **Modo de prevenção de exploits**, defina as seguintes configurações:
    - **Prevenir exploits de processos vulneráveis**.

        Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 reduzirá os riscos de exploração das vulnerabilidades dos processos da lista de processos protegidos.

        Se esta caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security 2.2 não protegerá os processos do computador contra exploits.

        Esta caixa é desmarcada por padrão.
        - **Encerrar no exploit**.

            Se este modo for selecionado, o Kaspersky Embedded Systems Security 2.2 encerrará um processo protegido após a detecção de uma tentativa de exploração se uma técnica ativa de redução de impacto tiver sido aplicada ao processo.
        - **Somente notificar processos violados**.

            Se este modo for selecionado, o Kaspersky Embedded Systems Security 2.2 relatará exploits exibindo uma janela de encerramento. O processo comprometido continua a ser executado.

            Se o Kaspersky Embedded Systems Security 2.2 detectar um exploit em um processo crítico enquanto o aplicativo estiver em execução no modo **Encerrar no exploit**, o componente será forçado a alternar para o modo **Somente notificar processos que tenham sofrido abuso**.

5. Na seção **Ações de prevenção**, defina as seguintes configurações:
   - **Notificar processos violados por meio do Serviço de terminal.**

     Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 exibirá uma janela do terminal com uma descrição explicando por que a proteção foi ativada e uma indicação do processo no qual uma tentativa de exploit foi detectada.

     Se a caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security 2.2 exibirá uma janela do terminal quando uma tentativa de exploit ou o encerramento de um processo comprometido forem detectados. Uma janela de terminal é exibida, independentemente do status do Kaspersky Security Exploit Prevention Service. A caixa de seleção é selecionada por padrão.
   - **Prevenir exploits de processos vulneráveis, mesmo com o Kaspersky Security Service desativado**.

     Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 reduzirá o risco de exploração de vulnerabilidades nos processos que já foram iniciados, mesmo que o Kaspersky Security Service esteja em execução. O Kaspersky Embedded Systems Security 2.2 não protegerá os processos adicionados depois que o Kaspersky Security Service for interrompido. Depois que o serviço for iniciado, a redução do impacto de exploits será interrompida para todos os processos.

     Se esta caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security 2.2 não protegerá os processos contra exploits quando o Kaspersky Security Service for interrompido.

     A caixa de seleção é selecionada por padrão.
6. Clique em **OK**.

O Kaspersky Embedded Systems Security 2.2 salva e aplica as configurações de proteção da memória do processo definidas.

Adição de um processo para proteção

O componente Prevenção de Exploits protege vários processos por padrão. Você pode excluir processos do escopo da proteção desmarcando as caixas correspondentes na lista.

► *Para adicionar um processo à lista de processos protegidos:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Proteção do Computador em Tempo Real**, clique no botão **Configurações** no bloco **Prevenção de Exploits**.

   A janela **Prevenção de Exploits** é exibida.

4. Na guia **Processos protegidos**, clique no botão **Procurar**.

   A janela do Microsoft Windows Explorer é exibida.

5. Selecione o processo que você deseja adicionar à lista.
6. Clique no botão **Abrir**.

   O nome de processo é exibido na linha.

7. Clique no botão **Adicionar**.

   O processo será adicionado à lista de processos protegidos.

8. Selecione o processo adicionado e clique em **Definir técnicas de prevenção de exploits**.

   A janela **Definir técnicas de prevenção de exploits** é exibida.

9. Selecione uma das opções para aplicar as técnicas de redução de impacto:
   - **Aplicar todas as técnicas de prevenção de exploits disponíveis**.

     Se esta opção for selecionada, a lista não poderá ser editada. Todas as técnicas disponíveis para um processo são aplicadas por padrão.

   - **Aplicar técnicas de prevenção de exploits listadas para o processo**.

     Se esta opção for selecionada, é possível editar a lista de técnicas de redução de impacto aplicadas:

     a. Marque as caixas de verificação ao lado das técnicas que você deseja aplicar para proteger o processo selecionado.
     b. Marque ou desmarque a caixa de seleção **Aplicar técnica de Redução de superfície de ataque**.

10. Defina as configurações da técnica de Redução de superfície de ataque:
    - Digite os nomes dos módulos cuja inicialização será bloqueada do processo protegido no campo **Negar módulos**.
    - No campo **Não negar módulos se iniciados na Área de Internet**, marque as caixas de seleção ao lado das opções sob as quais você deseja permitir que módulos sejam iniciados:
      - Internet
      - Intranet local
      - Sites confiáveis
      - Sites restritos
      - Computador

    > Essas configurações são aplicáveis apenas ao Internet Explorer®.

11. Clique em **OK**.

O processo é adicionado ao escopo da proteção da tarefa.

Técnicas de prevenção de exploits

Tabela 34. Técnicas de prevenção de exploits

Técnica de prevenção de exploits	Descrição
Prevenção Contra Execução de Dados (DEP, Data Execution Prevention)	A prevenção contra execução de dados bloqueia a execução do código arbitrário em áreas protegidas da memória.
Randomização do Layout do Espaço de Endereço (ASLR, Address Space Layout Randomization)	Altera o layout das estruturas de dados no espaço do endereço do processo.
Proteção contra Substituição do Gerenciador de Exceção Estruturada (SEHOP, Structured Exception Handler Overwrite Protection)	Substituição de registros de exceção ou substituição do gerenciador de exceção.
Alocação de Página Nula	Prevenção contra o redirecionamento do ponteiro nulo.
Verificação de Chamada de Rede LoadLibrary (Anti-ROP)	Proteção contra carregamento de DLLs de caminhos de rede.
Pilha Executável (Anti-ROP)	Bloqueio de execução não autorizada de áreas da pilha.
Verificação Anti-RET (Anti-ROP)	Verifica se a instrução CALL foi invocada de maneira segura.
Articulação Anti-Stack (Anti-ROP)	Proteção contra a relocalização do ponteiro de pilha ESP para um endereço executável.
Monitor de Acesso à Tabela de Endereço de Exportação (Monitor de Acesso EAT e Monitor de Acesso EAT através de Registrador de Depuração)	Proteção de acesso à leitura para a tabela de endereços de exportação para o kernel32.dll, kernelbase.dll e ntdll.dll
Alocação de heapspray (Heapspray)	Proteção contra a alocação de memória para executar um código malicioso.
Simulação do Fluxo de Execução (Contra Programação Direcionada por Retorno)	Detecção de cadeias suspeitas de instruções (possível gadget ROP) no componente de API do Windows.
Monitor de Chamada de Perfil de Intervalo (Proteção do Driver de Função Auxiliar (AFDP, Ancillary Function Driver Protection))	Proteção contra o escalamento de privilégios por uma vulnerabilidade no driver AFD (execução de código arbitrário no anel 0 através de uma chamada QueryIntervalProfile).
Redução da Superfície de Ataque (ASR)	Bloqueio da inicialização de suplementos vulneráveis por meio do processo protegido.
Contra o esvaziamento do processo (Hollowing)	Proteção contra criação e execução de cópias maliciosas de processos confiáveis.
Contra AtomBombing (APC)	Exploração da tabela de átomo global via Chamadas de Procedimento Assíncrono (APC).
Contra CreateRemoteThread (RThreadLocal)	Outro processo criou uma thread no processo protegido.
Contra CreateRemoteThread (RThreadRemote)	O processo protegido criou uma thread em outro processo.

Controle de Atividades Locais

Esta seção fornece informações sobre a funcionalidade do Kaspersky Embedded Systems Security 2.2 que controla inicializações de aplicativos, conexões de dispositivos externos via USB e Firewall do Windows.

Neste capítulo

Gerenciando a inicialização de aplicativos do Kaspersky Security Center

Você pode permitir ou negar a inicialização de aplicativos em todos os computadores dentro da rede corporativa criando listas comuns de regras de Controle de Inicialização de Aplicativos do lado do Kaspersky Security Center para grupos de computadores.

Nesta seção

Utilização de um perfil para configurar tarefas de Controle de Inicialização de Aplicativos em uma política do Kaspersky Security Center

As regras de Controle de Inicialização de Aplicativos configuradas na política são aplicadas a todos os computadores dentro do grupo de administração. Se um grupo de administração incluir computadores de vários tipos, as listas personalizadas de regras podem ser necessárias para o Controle de Inicialização de Aplicativos em cada computador. Você pode usar *perfis de política* para aplicar políticas diferentes a computadores dentro de um grupo de administração único.

Recomenda-se aplicar perfis de política para definir regras de Controle de Inicialização de Aplicativos para tipos de computadores diferentes dentro de um único grupo de administração regido por uma política unificada. Isto permite otimizar uma proteção do computador desde que as regras especificadas abranjam somente aquelas inicializações de aplicativos que são típicas para este exato tipo de computador.

Os perfis de política são aplicados a computadores do grupo de administração de acordo com as *marcas* atribuídas a eles. Você pode configurar um perfil de política para todos os computadores do grupo, que possuem uma única tag.

Informações detalhadas sobre marcas e perfis de política bem como as instruções sobre a utilização deles são fornecidas na *Ajuda do Kaspersky Security Center*.

► *Para aplicar um perfil de política à tarefa de Controle de Inicialização de Aplicativos:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados**. Expanda o grupo de administração para o qual você deseja configurar os perfis de política do aplicativo.
2. Atribua tags a cada computador dentro do grupo de administração de acordo com o tipo de computador. Para isso, execute as seguintes ações:
   - No painel de detalhes do grupo de administração selecionado, abra a guia **Dispositivos** e selecione o computador para o qual você deseja atribuir tags. Na janela **Propriedades: <Nome do computador>** do computador selecionado, selecione a seção **Tags** e crie uma lista de tags. Clique em **OK**.
3. Crie um perfil de política e configure o seu aplicativo para proteger computadores dentro do grupo de administração. Para isso, execute as seguintes ações:
   - No painel de detalhes do grupo de administração selecionado, abra a guia **Políticas** e selecione a política para a qual você deseja configurar os perfis do aplicativo. Na janela **Propriedades: <Nome da política>** da política selecionada, abra a seção **Perfis de política** e clique no botão **Adicionar** para criar um novo perfil. A janela **Propriedades: <Nome do perfil>** é exibida. Faça o seguinte:
     a. Na seção **Regras de ativação**, configure o escopo do aplicativo do perfil e especifique as condições nas quais o perfil será ativado.
     b. Na seção **Controle de inicialização de aplicativos**, configure as listas de regras de Controle de inicialização de aplicativos para o perfil que você está editando.
     c. Clique em **OK**.
4. Na janela **Propriedades: <Nome da política>**, clique em **OK**.

O perfil configurado será aplicado na política relacionada à tarefa de Controle de inicialização de aplicativos.

Definição de configurações da tarefa de Controle de Inicialização de Aplicativos

É possível alterar as configurações padrão da tarefa de Controle de Inicialização de Aplicativos (consulte a tabela abaixo).

Tabela 35. Configurações de tarefa de Controle de Inicialização de Aplicativos por padrão

Configuração	Valor padrão	Descrição
Modo da tarefa	**Somente estatísticas**. A tarefa registra eventos de inicialização e bloqueio do aplicativo com base nas regras definidas. A inicialização do aplicativo não é de fato negada.	Você pode selecionar o modo **Ativa** para a proteção do computador após a lista final de regras ser gerada.
Gerenciamento de regras	**Substituir regras locais por regras de política**	É possível selecionar um modo em que regras especificadas em uma política sejam aplicadas em conjunto com as regras no computador local.
Escopo de uso das regras	A tarefa controla a inicialização de arquivos executáveis, scripts e pacotes MSI.	É possível especificar tipos de arquivos para os quais a inicialização é controlada por regras.
Uso da KSN	Dados na reputação do aplicativo na KSN não são utilizados.	É possível usar os dados da reputação do aplicativo da KSN ao executar uma tarefa de Controle de Inicialização de Aplicativos.
Permitir distribuição automática de software para aplicativos e pacotes listados	Não aplicado.	É possível permitir a distribuição de software usando os instaladores e aplicativos especificados nas configurações. Por padrão, a distribuição de software só é permitida com a utilização do serviço do Windows Installer.
Sempre permitir distribuição de software via Windows Installer	Aplicada.	É possível permitir qualquer instalação ou atualização de software se as operações forem executadas via Windows Installer.
Negar a inicialização de intepretadores de comando sem comando a ser executado	Não aplicado.	Você pode negar a inicialização de interpretadores de comando sem comando a ser executado.
Início da tarefa	A primeira execução não está programada.	A tarefa de Controle de Inicialização de Aplicativos não é iniciada automaticamente no momento da inicialização do Kaspersky Embedded Systems Security 2.2. É possível iniciar a tarefa manualmente ou configurar um início programado.

► *Para definir as configurações gerais da tarefa de Controle de inicialização de Aplicativos, siga as etapas a seguir:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Controle de Atividades Locais**, clique no botão **Configurações** na seção **Controle de Inicialização de Aplicativos**.

   A janela **Controle de Inicialização de Aplicativos** é exibida.
4. Na guia **Geral**, selecione as seguintes configurações na seção **Modo**:

   Na lista suspensa **Modo da tarefa**, especifique o modo de operação de tarefa.

   Nesta lista suspensa você pode selecionar um modo de tarefa de Controle de inicialização de aplicativos:

   - **Ativa**. O Kaspersky Embedded Systems Security 2.2 usa as regras especificadas para monitorar qualquer aplicativo que esteja sendo executado.
   - **Somente estatísticas**. O Kaspersky Embedded Systems Security 2.2 não usa as regras especificadas para monitorar a inicialização de aplicativos, mas, ao invés disso, somente registra informações sobre essas inicializações no log de tarefas. A inicialização de todos os programas é permitida. Você pode usar este modo para gerar uma lista de regras de Controle de inicialização de aplicativos com base em informações registradas no log de tarefas.

   Por padrão, a tarefa de Controle de Inicialização de Aplicativos é executada no modo **Somente estatísticas**.

   - Desmarque ou selecione a caixa de seleção **Repetir ação da primeira inicialização de arquivo em todas as inicializações subsequentes deste arquivo**.

   A caixa ativa ou desativa o controle de inicialização para as segundas e subsequentes tentativas de iniciar aplicativos que se baseiam nas informações de incidente armazenadas em cache.

   Se a caixa estiver selecionada, o Kaspersky Embedded Systems Security 2.2 permitirá ou negará um reinício do aplicativo com base na conclusão que a tarefa havia enviado na primeira inicialização deste aplicativo. Por exemplo, se a primeira inicialização de aplicativo foi permitida pelas regras, as informações sobre esta ação serão armazenadas em cache e a segunda e todas as reinicializações subsequentes também serão permitidas, sem qualquer verificação adicional.

Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 analisará um aplicativo em cada tentativa de inicialização dele.

A caixa de seleção é selecionada por padrão.

- Desmarque ou selecione a caixa **Negar a inicialização de interpretadores de comando sem comando a ser executado**.

  Se a caixa for selecionada, o Kaspersky Embedded Systems Security 2.2 nega a inicialização do interpretador da linha de comando, mesmo se a inicialização do interpretador seja permitida. A linha de comando sem comando só pode ser inicializada se ambas as condições forem satisfeitas:

  - A inicialização do interpretador da linha de comando é permitida.
  - O comando executado é permitido.

  Se a caixa for desmarcada, o Kaspersky Embedded Systems Security 2.2 só considera as regras de permissão para a inicialização da linha de comando. A inicialização é negada se nenhuma regra de permissão for aplicada ou o processo executável não tiver status confiável na KSN. Se a regra de permissão for aplicada ou se o processo tiver status confiável na KSN, a linha de comando pode ser inicializada com ou sem comando a ser executado.

  O Kaspersky Embedded Systems Security 2.2 reconhece os seguintes interpretadores da linha de comando:

  - cmd.exe
  - powershell.exe
  - python.exe
  - perl.exe

5. Na seção **Regras**, defina as configurações para as regras de aplicação:

   a. Clique no botão **Lista de regras** para adicionar as regras de permissão para o controle de inicialização de tarefa.

   O Kaspersky Embedded Systems Security 2.2 não reconhece caminhos que contêm barras "/". Use a barra invertida "\" para inserir o caminho corretamente.

   b. Selecione o modo para a aplicação das regras:

   - **Substituir regras locais por regras de política**.

     O aplicativo aplica a lista de regras especificada na política para o controle centralizado de inicialização de aplicativos em um grupo de computadores. As listas de regras locais não podem ser criadas, editas ou aplicadas.

   - **Adicionar regras de política às regras locais**.

     O aplicativo aplica a lista de regras especificada em uma política junto com as listas de regra locais. É possível editar as listas de regras locais usando oa tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos.

   Por padrão, o Kaspersky Embedded Systems Security 2.2 aplica duas regras predefinidas que permitem uma lista de scripts, pacotes MSI e arquivos de inicialização com base em um certificado.

6. Na seção **Escopo de uso das regras**, especifique as seguintes configurações:

- **Aplicar regras a arquivos executáveis**.

  A caixa de seleção ativa/desativa o controle da inicialização de arquivos executáveis de programas.

  Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security 2.2 permitirá ou bloqueará a inicialização de arquivos executáveis de programas usando as regras especificadas cujas configurações indiquem Arquivos executáveis como o escopo.

  Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 não controlará a inicialização de arquivos executáveis de programas usando regras especificadas. A inicialização de arquivos executáveis de programas é permitida.

  A caixa de seleção é selecionada por padrão.

- **Monitorar carregamento dos módulos DLL**.

  A caixa ativa/desativa o monitoramento do carregamento dos módulos DLL

  Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security 2.2 permitirá ou bloqueará downloads de módulos DLL usando as regras especificadas cujas configurações indicam Arquivos executáveis como o escopo.

  Se esta caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 não monitorará os downloads de módulos DLL usando as regras especificadas. É permitido o download de módulos DLL.

  A caixa estará ativa se a caixa se seleção Aplicar regras a arquivos executáveis estiver selecionada.

  Esta caixa é desmarcada por padrão.

  O monitoramento de download dos módulos DLL pode afetar o desempenho do sistema operacional.

- **Aplicar regras a scripts e pacotes MSI**.

  A caixa ativa/desativa a inicialização de scripts e pacotes MSI.

  Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security 2.2 permitirá ou bloqueará a execução de scripts e pacotes MSI usando as regras especificadas cujas configurações indicam Scripts e pacotes MSI como o escopo.

  Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 não controlará a inicialização de scripts e pacotes MSI usando regras especificadas. A inicialização de scripts e pacotes MSI é permitida.

  A caixa de seleção é selecionada por padrão.

7. Na seção **Uso da KSN**, defina as seguintes configurações de inicialização de aplicativo:

- **Negar aplicativos não confiáveis pela KSN**.

  A caixa de seleção ativa ou desativa o Controle de Inicialização de Aplicativos segundo a sua reputação na KSN.

  Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security 2.2 bloqueará a execução de qualquer aplicativo que tiver o status não confiável na KSN. As regras de permissão de Controle de inicialização de aplicativos que se aplicam a aplicativos não confiáveis da KSN não serão acionadas. A seleção da caixa fornece proteção adicional contra malware.

Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 não considerará a reputação de programas não confiáveis na KSN e permitirá ou bloqueará a inicialização conforme as regras que se aplicam a esses programas.

Esta caixa é desmarcada por padrão.

- **Permitir aplicativos confiáveis pela KSN**.

  A caixa de seleção ativa ou desativa o Controle de Inicialização de Aplicativos segundo a sua reputação na KSN.

  Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security 2.2 permitirá que aplicativos sejam executados se tiverem status confiável na KSN. Negar regras de Controle de Inicialização de Aplicativos que são aplicadas aos aplicativos confiáveis na KSN tem uma maior prioridade: se o aplicativo for considerado confiável pelos serviços da KSN, a inicialização desse aplicativo será negada.

  Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 não considerará a reputação de programas confiáveis na KSN e permitirá ou bloqueará a inicialização conforme as regras que se aplicam a esses programas.

  Esta caixa é desmarcada por padrão.

- Os usuários e/ou grupos de usuário permitiram a inicialização de aplicativos confiáveis na KSN.

8. Na guia **Controle de distribuição de software**, defina as configurações do controle de distribuição de aplicativos (consulte a seção "Configuração do Controle de Distribuição de Software" na página 183).
9. Na guia **Gerenciamento da tarefa**, defina as configurações de início da tarefa agendada (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 122).
10. Clique em **OK** na janela **Configurações de tarefa**.

O Kaspersky Embedded Systems 2.2 aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora quando as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de tarefas.

Sobre o Controle de Distribuição de Software

A geração de regras de controle de inicialização de aplicativos pode ser complicada se você também precisar considerar o controle de distribuição de software em um computador protegido. Por exemplo, para aqueles computadores em que as atualizações automáticas periódicas do software instalado ocorrem. Nesse caso, ele é necessário para atualizar a lista de regras de permissão após cada atualização de software para que arquivos recém-criados sejam considerados nas configurações da tarefa de Controle de Inicialização de Aplicativos. Para simplificar o controle de inicialização nos cenários de distribuição de software, você pode usar o subsistema de Controle de Inicialização de Aplicativos.

Um *pacote de distribuição de software* (ou “um pacote”) representa um aplicativo de software a ser instalado em um computador. Cada pacote contém pelo menos um aplicativo e também pode conter arquivos individuais, atualizações, ou até um comando individual, além dos aplicativos, particularmente ao instalar um aplicativo de software ou atualização.

O subsistema de Controle de Distribuição de Software é implementado como uma lista adicional de exclusões. Quando você adiciona um pacote de distribuição de software a esta lista, o aplicativo permitirá a descompressão destes pacotes confiáveis e o início automático do software criado ou modificado por um pacote de confiança. Os arquivos extraídos podem herdar o atributo confiável de um pacote de distribuição primária. Um *pacote de distribuição primária* é um pacote que foi adicionado à lista de exclusões de Controle de Distribuição de Software pelo usuário e que se tornou um pacote confiável.

O Kaspersky Embedded Systems Security 2.2 controla apenas ciclos completos de distribuição de software. O aplicativo não pode processar corretamente a inicialização de arquivos modificados por um pacote confiável se, quando o pacote for iniciado pela primeira vez, o controle de distribuição de software estiver desligado ou o componente Controle de Inicialização de Aplicativos não estiver instalado.

O controle de distribuição de software não está disponível se a caixa **Aplicar regras a arquivos executáveis** for desmarcada nas configurações da tarefa de Controle de Inicialização de Aplicativos.

Cache de distribuição de software

O Kaspersky Embedded Systems Security 2.2 estabelece a conexão entre pacotes confiáveis e arquivos criados durante o procedimento de distribuição de software com a ajuda da *cache de distribuição de software* gerada dinamicamente (ou “cache de distribuição”). Quando o primeiro pacote é iniciado, o Kaspersky Embedded Systems Security 2.2 detecta todos os arquivos criados durante o processo de distribuição de software do pacote e armazena as somas de verificação dos arquivos e os caminhos na cache de distribuição. Posteriormente, é permitida a inicialização de todos os arquivos armazenados em cache de distribuição por padrão.

Você não pode rever, limpar ou modificar manualmente a cache de distribuição por meio da interface do usuário. A cache é preenchida e controlada pelo Kaspersky Embedded Systems Security 2.2.

Você pode exportar a cache de distribuição no arquivo de configuração (no formato XML) e também limpar a cache usando opções da linha de comando.

► *Para exportar a cache de distribuição para um arquivo de configuração, execute o seguinte comando:*

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

► *Para limpar a cache de distribuição, execute o seguinte comando:*

```
kavshell appcontrol /config /clearsdc
```

O Kaspersky Embedded Systems Security 2.2 atualiza a cache de distribuição a cada 24 horas. Se o caminho completo ou a soma de verificação de um arquivo anteriormente permitido for alterado, o aplicativo exclui o registro de tal arquivo da cache de distribuição. Se a tarefa de Controle de Inicialização de Aplicativos for iniciada no modo Ativa, inicializações posteriores desse arquivo serão bloqueadas.

Processamento de arquivos extraídos

O atributo confiável para todos os arquivos extraídos do pacote confiável é herdado na primeira inicialização do pacote. Se você desmarcar a caixa após a primeira inicialização, a herança de todos os arquivos extraídos do pacote ainda será mantida. Para reinicializar a herança aplicada inicialmente a todos os arquivos extraídos, será necessário limpar a cache de distribuição e desmarcar a caixa **Permitir a inicialização para todos os arquivos desta cadeia de extração do pacote de distribuição** antes de iniciar o pacote de distribuição confiável novamente.

Os arquivos e pacotes extraídos, criados por um pacote de distribuição primária confiável, adquirem o atributo confiável já que suas somas de verificação são adicionadas à cache de distribuição quando o pacote de distribuição de software da lista de exclusão é aberto pela primeira vez. Portanto, o próprio pacote de distribuição e todos os arquivos extraídos de tal pacote também serão confiáveis. Por padrão, o número de níveis de herança do atributo confiável é ilimitado.

O atributo confiável será mantido pelos arquivos extraídos depois do reinício do sistema operacional.

O processamento de arquivos é definido nas configurações de Controle de Distribuição de Software (consulte a seção "Configuração do controle de distribuição de software" na página 183) selecionando ou desmarcando a caixa **Permitir a inicialização para todos os arquivos desta cadeia de extração do pacote de distribuição**.

Por exemplo, você adiciona um pacote test.msi contendo vários outros pacotes e aplicativos à lista de exclusões seleciona a caixa. Nesse caso, todos os pacotes e aplicativos contidos no pacote test.msi podem ser executados ou extraídos se contiverem outros arquivos. Este cenário funciona para arquivos extraídos em todos os níveis aninhados.

Se você adicionar um pacote test.msi à lista de exclusões e desmarcar a caixa **Permitir a inicialização para todos os arquivos desta cadeia de extração do pacote de distribuição**, o aplicativo destinará o atributo confiável apenas aos pacotes e arquivos executáveis extraídos diretamente de um pacote confiável primário (aninhado ao primeiro nível). As somas de verificação de tais arquivos são armazenadas em cache de distribuição. Todos os arquivos aninhados ao segundo nível e além serão bloqueados pelo princípio de Negação padrão.

Interação com a lista de regras de controle de inicialização de aplicativos

A lista de pacotes confiáveis do subsistema de controle de distribuição de software é uma lista de exclusões que amplifica, mas não substitui a lista geral de regras de controle de inicialização de aplicativos.

As regras de negação de controle de inicialização de aplicativos têm a prioridade mais alta: a descompressão de pacotes confiáveis e a inicialização de arquivos novos ou modificados serão bloqueadas caso tais pacotes e arquivos forem afetados pelas regras de negação de controle de inicialização de aplicativos.

As exclusões do controle de distribuição de software são aplicadas tanto para pacotes confiáveis quanto para arquivos criados ou modificados por tais pacotes, caso nenhuma regra de negação de controle de inicialização de aplicativos seja aplicada àqueles pacotes e arquivos.

Usar conclusões da KSN

As conclusões não confiáveis da KSN têm uma prioridade mais alta do que as exclusões do controle de distribuição de software: a descompressão de um pacote confiável ou a inicialização de arquivos criados e modificados por tal pacote será bloqueada se uma conclusão não confiável for recebida da KSN para tais arquivos.

Configuração do controle de distribuição de software

► *Para adicionar um pacote de distribuição confiável, faça o seguinte:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações

do aplicativo do Kaspersky Security Center" na página 101).

> Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Controle de Atividades Locais**, clique no botão **Configurações** na seção **Controle de Inicialização de Aplicativos**.

   A janela **Controle de Inicialização de Aplicativos** é exibida.

4. Na guia selecionada, marque a caixa de seleção **Permitir distribuição automática de software para aplicativos e pacotes listados**.

   A caixa de seleção ativa e desativa a criação automática de exclusões para todos os arquivos iniciados usando os pacotes de distribuição especificados na lista.

   Se a caixa de seleção for marcada, o aplicativo permite automaticamente que os arquivos nos pacotes de distribuição confiáveis sejam inicializados. A lista de aplicações e pacotes de distribuição permitidos para inicialização podem ser editados.

   Se a caixa de seleção for desmarcada, o aplicativo não aplicará as exclusões específicas na lista.

   Esta caixa é desmarcada por padrão.

> É possível selecionar **Permitir distribuição automática de software para aplicativos e pacotes listados** se a caixa de seleção **Aplicar regras a arquivos executáveis** estiver marcada nas configurações da tarefa de **Controle de Inicialização de Aplicativos**.

5. Desmarque a caixa de seleção **Sempre permitir distribuição de software via Windows Installer**, se necessário.

   A caixa de seleção ativa e desativa a criação automática de exclusões para todos os arquivos executados através do Windows Installer.

   Se a caixa de seleção for marcada, o aplicativo sempre permitirá que arquivos instalados através do Windows Installer sejam iniciados.

   Se a caixa de seleção for desmarcada, o aplicativo não será permitido incondicionalmente, mesmo se iniciado através do Windows Installer.

   A caixa de seleção é selecionada por padrão.

   A caixa de seleção não é editável se a caixa **Permitir distribuição automática de software para pacotes listados** não estiver marcada.

> Desmarcar a caixa de seleção **Sempre permitir distribuição de software via Windows Installer** só é recomendado se for absolutamente necessário. Desativar essa função pode causar problemas na atualização dos arquivos do sistema operacional e também evitar que arquivos extraídos de um pacote de distribuição sejam iniciados.

6. Se necessário, marque a caixa de seleção **Sempre permitir distribuição de software via SCCM usando o Background Intelligent Transfer Service**.

   A caixa de seleção ativa e desativa a distribuição automática de software usando o System Center Configuration Manager.

   Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security 2.2 automaticamente permitirá a implantação do Microsoft Windows usando o System Center Configuration Manager. O aplicativo permite a distribuição de software apenas através do Serviço de transferência inteligente em segundo plano.

O aplicativo controla a inicialização dos objetos com as seguintes extensões:

- .exe
- .msi

Esta caixa é desmarcada por padrão.

> O aplicativo controla o ciclo de distribuição de software no computador, da entrega do pacote à instalação/atualização. O aplicativo não controla processos se algum dos estágios da distribuição tiver sido executado antes da instalação do aplicativo no computador.

7. Para editar a lista de pacotes de distribuição confiáveis, clique em **Alterar lista de pacotes** e selecione um dos seguintes métodos na janela exibida:

- **Adicionar um pacote de distribuição**.
  a. Clique no botão **Procurar** e selecione um arquivo executável ou pacote de distribuição.

     A seção **Critérios de confiança** é automaticamente preenchida com os dados sobre o arquivo selecionado.
  b. Desmarque ou selecione a caixa **Permitir a inicialização para todos os arquivos desta cadeia de extração do pacote de distribuição**.
  c. Selecione uma das duas opções disponíveis para os critérios a serem usados para determinar se um arquivo ou pacote de distribuição é confiável:
     - **Usar certificado digital**

       Se esta opção estiver selecionada, a presença de um certificado digital será especificada como o critério de acionamento de regra nas configurações das regras de permissão geradas recentemente para o Controle de inicialização de aplicativos. O aplicativo permitirá agora a inicialização de programas iniciados usando arquivos com um certificado digital. Esta opção é recomendada se você quiser permitir a inicialização de qualquer aplicativo que seja confiável no sistema operacional.
     - **Usar hash SHA256**

       Se esta opção estiver selecionada, o valor da soma de verificação do arquivo, usado para gerar a regra, será especificado como o critério de acionamento de regra nas configurações das regras de permissão geradas recentemente para o Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com o valor da soma de verificação especificado.

       Esta opção é recomendada para casos quando as regras geradas são necessárias para alcançar o nível de segurança mais alto: a soma de verificação do SHA256 pode ser aplicada como um ID único de arquivo. O uso da soma de verificação do SHA256 como critério para acionamento de regras restringe o escopo de uso da regra em até um arquivo.

       Esta opção é selecionada por padrão.
- **Adicionar diversos pacotes de distribuição por hash**.

  > É possível selecionar um número ilimitado de arquivos executáveis e pacotes de distribuição e adicioná-los à lista ao mesmo tempo. O Kaspersky Embedded Systems Security 2.2 examina o hash e permite que o sistema operacional inicie os arquivos especificados.
- **Alterar pacote selecionado**.

Use esta opção para selecionar um arquivo executável ou pacote de distribuição diferente, ou para alterar os critérios de confiança.

- **Importar lista de pacotes de distribuição do arquivo**.

  É possível importar a lista de pacotes de distribuição confiáveis do arquivo de configuração. O arquivo reconhecido pelo Kaspersky Embedded Systems Security 2.2 deve satisfazer os seguintes parâmetros:

  - O arquivo tem uma extensão de texto.
  - O arquivo contém informações estruturadas como uma lista de linhas, onde cada linha inclui dados para um dos arquivos confiáveis.
  - O arquivo deve conter uma lista em um dos seguintes formatos:
    - <nome do arquivo>:<hash SHA256>.
    - <hash SHA256>*<nome do arquivo>.

  Na janela **Abrir**, especifique o arquivo de configuração que contém uma lista de pacotes de distribuição confiáveis.

8. Se quiser remover um aplicativo ou pacote de distribuição previamente adicionado da lista de confiáveis, clique no botão **Excluir pacotes de distribuição**. Arquivos extraídos não poderão ser executados.

   > Para evitar que arquivos extraídos sejam iniciados, desinstale o aplicativo no computador protegido ou crie uma regra de negação nas configurações da tarefa de Controle de Inicialização de Aplicativos.

9. Clique em **OK**.

As configurações recém-definidas foram salvas.

Ativar o modo de Permissão padrão

O modo de Permissão padrão permite que todos os aplicativos sejam inicializados se não estiverem bloqueados por regras ou pela conclusão não confiável da KSN. O modo de Permissão padrão pode ser ativado adicionando regras de permissão específicas. Você pode ativar a Permissão padrão para scripts ou para todos os arquivos executáveis.

► *Para adicionar uma regra de Permissão padrão:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

> Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Controle de Atividades Locais**, clique no botão **Configurações** no bloco **Controle de Inicialização de Aplicativos**.
4. Na guia **Geral**, clique no botão **Lista de regras**.

   A janela **Regras de controle de inicialização de aplicativos** é exibida.
5. Clique no botão **Adicionar** e no menu de contexto do botão selecione a opção **Adicionar uma regra**.

   A janela **Configurações de regra** é exibida.
6. No campo **Nome**, digite o nome da regra.
7. Na lista suspensa **Tipo**, selecione o tipo de regra **Permissão**.
8. Na lista suspensa **Escopo**, selecione o tipo de arquivo cuja execução será controlada pela regra:
   - **Arquivos executáveis** se deseja que a regra controle a inicialização de arquivos executáveis de aplicativos.
   - **Scripts e pacotes MSI** se deseja que a regra controle a inicialização de scripts e pacotes MSI.
9. Na seção **Critério para acionamento de regras**, selecione a opção **Caminho do arquivo**.
10. Insira a seguinte máscara: **?:**
11. Clique em **OK** na janela **Configurações de regra**.

O Kaspersky Embedded Systems Security 2.2 aplica o modo de Permissão padrão.

Sobre a geração de regras de Controle de inicialização de aplicativos para todos os computadores no Kaspersky Security Center

Você pode criar listas de regras de Controle de inicialização de aplicativos usando tarefas e políticas do Kaspersky Security Center para todos os computadores e grupos de computadores na rede corporativa ao mesmo tempo. Este cenário é recomendado se a rede corporativa não tiver uma máquina de referência e se você não puder criar uma lista comum de regras usando uma tarefa para gerar automaticamente regras de permissão com base nos aplicativos instalados na máquina de referência.

O componente Controle de Inicialização de Aplicativos é instalado com duas regras de permissão predefinidas:

- Regra de permissão para scripts e MSI com certificado confiável do sistema operacional.
- Regra de permissão para arquivos executáveis com certificado confiável do sistema operacional.

Você pode criar listas de regras de Controle de inicialização de aplicativos no lado do Kaspersky Security Center de duas maneiras:

- Usando uma tarefa de grupo de Gerador de Regras de Controle de Inicialização de Aplicativos para o Controle de Inicialização de Aplicativos.

  Quando este cenário é usado, uma tarefa de grupo gera sua própria lista de regras de Controle de inicialização de aplicativos para cada computador na rede e salva aquelas listas em um arquivo XML na pasta de rede compartilhada especificada. Você pode então importar manualmente a lista de regras criada na tarefa de Controle de inicialização de aplicativos da política do Kaspersky Security Center. É possível configurar uma política do Kaspersky Security Center para adicionar automaticamente as regras criadas à lista de regras do Controle de Inicialização de Aplicativos quando a tarefa de grupo de Gerador de Regras de Controle de Inicialização de Aplicativos é concluída.

Este cenário é recomendado quando é necessário criar listas da regra de Controle de inicialização de aplicativos a curto prazo. Recomenda-se configurar a inicialização programada da tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos somente se o escopo do aplicativo das regras de permissão incluir pastas, contendo arquivos certificadamente seguros.

> Antes de usar a política de Controle de inicialização de aplicativos, certifique-se de que todo computador protegido tenha acesso a uma pasta de rede compartilhada. Se a política da organização não prevê o uso de uma pasta de rede compartilhada na rede, recomenda-se começar a tarefa de Geradores de regras automatizadas para regras de controle do computador no grupo de computadores de teste ou em uma máquina modelo.

- Com base em um relatório sobre eventos de tarefa gerado no Kaspersky Security Center para a operação da tarefa de Controle de inicialização de aplicativos no modo **Somente estatísticas**.

  Quando este cenário for usado, o Kaspersky Embedded Systems Security 2.2 não nega inicializações de aplicativos, mas enquanto o Controle de Inicialização de Aplicativos é executado no modo **Somente estatísticas**, ele reporta todos as inicializações de aplicativos permitidas e negadas em toda a rede de computadores na seção **Eventos** do Kaspersky Security Center. O Kaspersky Security Center gera a lista unificada de eventos de inicializações de aplicativos negadas, com base no log de tarefas.

  Você precisa configurar o período de execução da tarefa para que todos os cenários possíveis de operação de computadores protegidos e de grupos de computadores e, pelo menos, um reinício sejam executados durante o período de tempo especificado. Em seguida, conforme as regras são adicionadas à tarefa de Controle de inicialização de aplicativos você pode importar dados sobre as inicializações de aplicativo do arquivo de relatório de evento salvo do Kaspersky Security Center (no formato TXT) e gerar regras de permissão de Controle de inicialização de aplicativos de tais aplicativos com base nestes dados.

  Este cenário é recomendado se uma rede corporativa incluir uma grande quantidade de computadores de tipos diferentes (consulte a seção “Utilização de um perfil para configurar tarefas de Controle de Inicialização de Aplicativos em uma política do Kaspersky Security Center” na página 175) (com um conjunto diferente de software instalado).

- Com base nos eventos de inicialização de aplicativos negados recebidos pelo Kaspersky Security Center, sem criar e importar um arquivo de configuração.

  Para usar esse recurso, a tarefa de Controle de Inicialização de Aplicativos no computador local deve estar em execução segundo uma política ativa do Kaspersky Security Center. Neste caso, todos os eventos no computador local são enviados para o Servidor de administração.

Recomenda-se atualizar a lista de regras quando há modificações no conjunto de aplicativos instalado nos computadores da rede (por exemplo, quando as atualizações são instaladas ou os sistemas operacionais são reinstalados). Recomenda-se usar a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos ou a política de Controle de Inicialização de Aplicativos no modo **Somente estatísticas**, executadas em computadores no grupo de administração de teste, para gerar uma lista atualizada de regras. O grupo de administração de teste inclui computadores necessários para a inicialização do teste de novos aplicativos antes que eles sejam instalados em computadores da rede.

Antes de adicionar regras de permissão, selecione um dos modos de aplicação de regra disponíveis (consulte a seção "Definição de configurações da tarefa de Controle de Inicialização de Aplicativos" na página 177). A lista das regras da política do Kaspersky Security Center exibe apenas as que são especificadas pela política, independentemente do modo de aplicação de regra. A lista de regras locais exibe todas as regras aplicadas - tanto para regras locais como as adicionadas através de uma política.

Nesta seção

Criação de regras de permissão dos eventos do Kaspersky Security Center

► *Para gerar as regras de permissão usando a opção "Criar regras de permissão para aplicativos de eventos do Kaspersky Security Center" no Controle de Inicialização de Aplicativos, faça o seguinte:*

1. No Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciado**.
2. Expanda o grupo de administração cujas configurações de política você deseja configurar e selecione a guia **Políticas** no painel de detalhes.
3. Selecione **Propriedades** no menu de contexto da política que você deseja configurar.

   A janela **Propriedades: <Nome da política>** é exibida.
4. Na seção **Controle de Atividades Locais**, clique no botão **Configurações** no bloco **Controle de Inicialização de Aplicativos**.
5. Na guia **Geral**, clique no botão **Lista de regras**.

   A janela **Regras de controle de inicialização de aplicativos** é exibida.
6. Clique no botão **Adicionar** e, no menu de contexto do botão, selecione **Criar regras de permissão para aplicativos de eventos do Kaspersky Security Center**.
7. Selecione o princípio para adicionar as regras à lista de regras de controle de inicialização de aplicativos criados anteriormente:
   - **Adicionar às regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
   - **Substituir as regras existentes** se deseja substituir as regras existentes com as importadas.
   - **Mesclar com as regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

   A janela **Gerar regras de controle de inicialização de aplicativos** é exibida.
8. Defina as seguintes configurações de solicitação:
   - **Endereço do Servidor de Administração**

- **Porta**
- **Usuário**
- **Senha**

9. Selecione os tipos de eventos em que deseja basear a tarefa de geração:
   - **Modo Somente estatísticas: inicialização do aplicativo negada**.
   - **Inicialização do aplicativo negada**.
10. Selecione o período do tempo na lista suspensa **Solicitação de eventos gerados no período**.
11. Clique no botão **Gerar regras**.
12. Clique no botão **Salvar** na janela **Regras de controle de inicialização de aplicativos**.

    A lista de regras na política de Controle de Inicialização de Aplicativos será preenchida com novas regras geradas com base em dados do sistema do computador com o Console de Administração do Kaspersky Security Center instalado.

    > Se a lista de regras de Controle de inicialização de aplicativos já estiver especificada na política, o Kaspersky Embedded Systems Security 2.2 adicionará as regras selecionadas dos eventos de bloqueio às regras já especificadas. As regras com o mesmo hash não serão adicionadas, pois todas as regras em uma lista devem ser únicas.

Importando o Controle de inicialização de aplicativos a partir de um arquivo XML

Você pode importar relatórios gerados após a conclusão da tarefa de grupo de Gerador de Regras de Controle de Inicialização de Aplicativos e aplicá-los como uma lista de regras de permissão na política que estiver configurando.

Quando a tarefa de grupo de Gerador de Regras de Controle de Inicialização de Aplicativos for concluída, o aplicativo exportará as regras de permissão criadas para arquivos XML salvos na pasta de rede compartilhada especificada. Cada arquivo com a lista de regras é criado com base na análise de arquivos executados e aplicativos iniciados em cada computador separado na rede corporativa. As listas contêm regras de permissão para arquivos e aplicativos cujo tipo corresponde ao tipo especificado na tarefa de grupo de Gerador de Regras de Controle de Inicialização de Aplicativos.

> O processo de definição das configurações dos componentes funcionais do Kaspersky Embedded Systems Security 2.2 no Kaspersky Security Center é similar à definição local das configurações destes componentes no Console do Aplicativo. As instruções detalhadas sobre como definir configurações da tarefa e funções do aplicativo são fornecidas nas seções relevantes do *Manual do Usuário do Kaspersky Embedded Systems Security 2.2*.

► *Para especificar regras de permissão para a inicialização do aplicativo para um grupo de computadores com base em uma lista de regras de permissão gerada automaticamente, siga as etapas a seguir.*

1. Na guia **Tarefas** no painel de controle do grupo de computadores que você está configurando, crie uma tarefa de grupo de Gerador de Regras de Controle de Inicialização de Aplicativos ou selecione uma tarefa existente.
2. Nas propriedades da tarefa de grupo de Gerador de Regras de Controle de Inicialização de Aplicativos

criada ou no assistente de tarefa, especifique as seguintes configurações:

- Na seção **Notificação**, defina as configurações para salvar o relatório de execução da tarefa.

  > Para obter instruções detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*

- Na seção **Configurações**, especifique os tipos de aplicativos cuja inicialização será permitida pelas regras criadas. Você pode editar o conteúdo das pastas que contêm aplicativos permitidos: excluir pastas padrão do escopo de tarefa ou adicionar novas pastas manualmente.
- Na seção **Opções**, especifique as operações de tarefa enquanto ela é executada e após sua conclusão. Especifique o critério com base no qual as regras serão geradas e o nome do arquivo ao qual estas regras serão exportadas.
- Na janela **Programação**, defina as configurações da programação da inicialização da tarefa.
- Na seção **Conta**, especifique a conta de usuário sob a qual a tarefa será executada.
- Na seção **Exclusões do escopo de tarefa**, especifique os grupos de computadores a serem excluídos do escopo da tarefa.

  > O Kaspersky Embedded Systems Security 2.2 não cria regras de permissão para aplicativos iniciados em computadores excluídos.

3. Na guia **Tarefas** no painel de controle do grupo de computadores sendo configurados, na lista de tarefas de grupo selecione o Gerador de Regras de Controle de Inicialização de Aplicativos que você criou e clique no botão **Iniciar** para iniciar a tarefa.

   Quando a tarefa é concluída, as listas de regras de permissão geradas automaticamente são salvas em uma pasta de rede compartilhada em arquivos XML.

   > Antes de usar a política de Controle de inicialização de aplicativos, certifique-se de que todo computador protegido tenha acesso a uma pasta de rede compartilhada. Se a política da organização não prevê o uso de uma pasta de rede compartilhada na rede, recomenda-se começar a tarefa de Geradores de regras automatizadas para regras de controle do computador no grupo de computadores de teste ou em uma máquina modelo.

4. Adicione as listas de regras de permissão geradas à tarefa de Controle de inicialização de aplicativos. Para fazer isso, nas propriedades da política que está sendo configurada, nas configurações de tarefa de Controle de inicialização de aplicativos:

   a. Na guia **Geral**, clique no botão **Lista de regras**.

      A janela **Regras de controle de inicialização de aplicativos** é exibida.

   b. Clique no botão **Adicionar** e na lista exibida selecione **Importar regras do arquivo XML**.

   c. Selecione o princípio para adicionar as regras de permissão geradas automaticamente à lista de regras de Controle de inicialização de aplicativos criadas anteriormente:

      - **Adicionar às regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
      - **Substituir as regras existentes** se deseja substituir as regras existentes com as importadas.

* **Mesclar com as regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

d. Na janela padrão do Microsoft Windows exibida, selecione arquivos XML criados após a conclusão da tarefa de grupo de Gerador de Regras de Controle de Inicialização de Aplicativos.

e. Clique em **OK** na janela **Regras de controle de inicialização de aplicativos** e na janela **Configurações de tarefa**.

5. Se você deseja aplicar as regras criadas para controlar a inicialização do aplicativo, na política nas propriedades da tarefa de Controle de Inicialização de Aplicativos selecione o modo de execução da tarefa **Ativa**.

Regras de permissão geradas automaticamente com base em execuções de tarefa em cada computador separado são aplicadas a todos os computadores de rede abrangidos pela política que está sendo configurada. Nestes computadores, o aplicativo permitirá a inicialização somente daqueles aplicativos para os quais as regras de permissão foram criadas.

Importando regras do arquivo de um relatório do Kaspersky Security Center sobre aplicativos bloqueados

Você pode importar dados sobre inicializações de aplicativo bloqueadas do relatório gerado no Kaspersky Security Center após a conclusão da tarefa de Controle de Inicialização de aplicativos no modo **Somente estatísticas** e usar estes dados para gerar uma lista de regras de permissão de Controle de Inicialização de Aplicativos na política que está sendo configurada.

Ao gerar o relatório sobre eventos que ocorrem durante uma tarefa de Controle de Inicialização de Aplicativos, você pode acompanhar os aplicativos cuja inicialização está bloqueada.

Ao importar dados do relatório sobre aplicativos bloqueados nas configurações de política, certifique-se de que a lista que está sendo usada contenha somente aplicativos cuja inicialização você deseja permitir.

► *Para especificar regras de permissão para a inicialização do aplicativo para um grupo de computadores com base no relatório de aplicativos bloqueados do Kaspersky Security Center, siga estas etapas:*

1. Nas propriedades de política nas configurações da tarefa de Controle de inicialização de aplicativos, selecione o modo de operação **Somente estatísticas**.
2. Nas propriedades de política na seção **Eventos**, certifique-se de que:
   * A guia **Eventos críticos** do evento Inicialização do aplicativo negada mostra um tempo de armazenamento de evento que excede o tempo planejado da operação de tarefa no modo **Somente estatísticas** (o valor padrão é 30 dias).

- A guia **Aviso** do evento *Somente estatísticas: inicialização do aplicativo negada* mostra um tempo de armazenamento de evento que excede o tempo planejado da operação de tarefa no modo **Somente estatísticas** (o valor padrão é 30 dias).

> Quando o período especificado na coluna **Tempo de armazenamento** é excedido, as informações sobre eventos registrados são excluídas e não são refletidas no arquivo de relatório. Antes de executar a tarefa de Controle de inicialização de aplicativos no modo **Somente estatísticas**, certifique-se de que o tempo de execução da tarefa não exceda o tempo de armazenamento configurado para os eventos especificados.

3. Após a tarefa ter sido concluída, exporte os eventos registrados para um arquivo TXT:
   a. Para isso, nas propriedades da tarefa de Controle de Inicialização de Aplicativos, expanda o nó **Logs e notificações**.
   b. No nó filho **Evento** crie uma seleção de eventos com base no critério *Bloqueado* para exibir os aplicativos cujo início será bloqueado pela tarefa de Controle de Inicialização de Aplicativos.
   c. No painel de detalhes da seleção, clique na lista **Exportar eventos** para arquivo para salvar o relatório de inicializações de aplicativos bloqueadas em um arquivo TXT.

> Antes de importar e aplicar o relatório gerado a uma política, certifique-se de que o relatório contenha somente dados sobre aqueles aplicativos cuja inicialização você deseja permitir.

4. Importe os dados sobre inicializações de aplicativos bloqueadas na tarefa de Controle de Inicialização de Aplicativos. Para fazer isso, nas propriedades da política nas configurações de tarefa de Controle de inicialização de aplicativos:
   a. Na guia **Geral**, clique no botão **Lista de regras**.

      A janela **Regras de controle de inicialização de aplicativos** é exibida.
   b. Clique no botão **Adicionar** e no menu de contexto do botão selecione **Importar dados de aplicativos bloqueados do relatório do Kaspersky Security Center**.
   c. Selecione o princípio para adicionar regras da lista criada com base no relatório do Kaspersky Security Center à lista de regras previamente configuradas de Controle de inicialização de aplicativos:
      - **Adicionar às regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
      - **Substituir as regras existentes** se deseja substituir as regras existentes com as importadas.
      - **Mesclar com as regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.
   d. Na janela padrão do Microsoft Windows exibida, selecione o arquivo TXT para o qual os eventos do relatório de inicializações de aplicativos bloqueadas foram exportados.
   e. Clique em **OK** na janela Regras de controle de inicialização de aplicativos e na janela **Configurações de tarefa**.

As regras criadas com base no relatório do Kaspersky Security Center sobre aplicativos bloqueados são adicionadas à lista de regras de controle de inicialização de aplicativos.

Gerenciando conexões de dispositivos por meio do Kaspersky Security Center

Você pode permitir ou restringir conexões de pen drives e de outros armazenamentos em massa para todos os computadores na rede ao gerar listas de controle do computador unificadas por meio do Kaspersky Security Center para os grupos dos computadores.

Nesta seção

Sobre a tarefa de Controle de Dispositivos

O Kaspersky Embedded Systems Security 2.2 controla o registro e uso dos armazenamentos em massa e unidades de CD/DVD para proteger o computador contra ameaças de segurança, que podem ocorrer no processo da troca de arquivos com pen drives ou outro tipo de dispositivo externo conectado via USB. O armazenamento em massa é um dispositivo externo que pode ser conectado a um computador para copiar ou armazenar arquivos.

O Kaspersky Embedded Systems Security 2.2 controla as seguintes conexões de dispositivos externos USB:

- Pen drives conectados por USB
- Unidades de CD/DVD-ROM
- Unidades de disquete conectadas por USB
- Dispositivos móveis MTP conectados por USB

O Kaspersky Embedded Systems Security 2.2 informa sobre todos os dispositivos conectados via USB com o evento correspondente nos logs de tarefa e de evento. Os detalhes do evento incluem o tipo de dispositivo e o caminho de conexão. Quando a tarefa de Controle de Dispositivos é iniciada, o Kaspersky Embedded Systems Security 2.2 verifica e lista todos os dispositivos conectados via USB. Você pode configurar as notificações na seção de configurações de notificação do Kaspersky Security Center.

A tarefa de Controle de Dispositivos monitora todas as tentativas de conexão de dispositivos externos a um computador protegido via USB e bloqueia a conexão se não houver regras de permissão para tais dispositivos. Após a conexão ser bloqueada, o dispositivo não fica disponível.

O aplicativo atribui um dos seguintes status a cada armazenamento em massa conectado:

- *Confiável*. O dispositivo para o qual você deseja permitir a troca de arquivos. Após a geração da lista de regras, o valor do caminho da instância do dispositivo será incluído no escopo de uso de pelo menos uma regra.

- *Não confiável*. Dispositivo para o qual você deseja restringir a troca de arquivos. O caminho da instância do dispositivo não está incluído em nenhum escopo de uso das regras de permissão.

Você pode criar regras de permissão para dispositivos externos para permitir a troca de dados usando a tarefa de Gerador de Regras de Controle de Dispositivos. Você também pode expandir o escopo de uso das regras já especificadas. Você não pode criar regras de permissão manualmente.

O Kaspersky Embedded Systems Security 2.2 identifica os armazenamentos em massa registrados pelo sistema usando o valor do *Caminho da instância do dispositivo*. O Caminho da instância do dispositivo é um recurso padrão especificado unicamente para cada dispositivo externo. O valor do Caminho da instância do dispositivo é especificado para cada dispositivo externo nas suas propriedades Windows e é automaticamente determinado pelo Kaspersky Embedded Systems Security 2.2 durante a geração de regras.

A tarefa de Controle de Dispositivos pode operar em dois modos:

- **Ativa**. O Kaspersky Embedded Systems Security 2.2 aplica regras para controlar a conexão de pen drives e outros dispositivos externos e permite ou bloqueia o uso de todos os dispositivos de acordo com o princípio Negação Padrão e as regras de permissão especificadas. O uso de dispositivos externos confiáveis é permitido. Por padrão, o uso de dispositivos externos não confiáveis é bloqueado.

  Se um dispositivo externo que você considera não confiável for conectado a um computador protegido antes que a tarefa de Controle de Dispositivos seja executada no modo Ativa, o dispositivo não será bloqueado pelo aplicativo. Recomendamos que desconecte o dispositivo não confiável manualmente ou reinicie o computador. Caso contrário, o princípio de Negação Padrão não será aplicado ao dispositivo.

- **Somente estatísticas**. O Kaspersky Embedded Systems Security 2.2 não controla a conexão de pen drives e outros dispositivos externos, só registra em log informações sobre a conexão e o registro de dispositivos externos em um computador protegido e sobre as regras de permissão de Controle de Dispositivos acionadas pelos dispositivos conectados. O uso de todos os dispositivos externos é permitido. Este modo está definido por padrão.

  Você pode aplicar este modo para geração de regras com base nas informações registradas em log durante a execução da tarefa.

Sobre a geração de regras de Controle de dispositivos para todos os computadores por meio do Kaspersky Security Center

Você pode criar listas de regras de Controle de dispositivos usando tarefas do Kaspersky Security Center para todos os computadores e os grupos de computadores na rede corporativa ao mesmo tempo.

Você pode criar listas de regras de Controle de dispositivos no lado do Kaspersky Security Center de duas maneiras:

- Usando a tarefa de grupo de Gerador de Regras de Controle de Dispositivos.

  Segundo este cenário, a tarefa de grupo gera listas de regras com base nos dados de sistema de cada computador sobre todos os dispositivos de armazenamento em massa que já foram conectados a computadores protegidos. A tarefa também permite todos os dispositivos de armazenamento em massa conectados no momento da execução da tarefa. Após a conclusão da tarefa de grupo o Kaspersky Embedded Systems Security 2.2 gera listas de regras de permissão para todos os dispositivos de armazenamento em massa registrados na rede e salva tais listas em um arquivo XML em uma pasta especificada. Em seguida, você pode importar manualmente regras geradas nas configurações de política de Controle de dispositivos. Diferentemente de uma tarefa em um computador local, a política não permite configurar a adição automática das regras criadas à lista de regras de Controle de dispositivos quando a tarefa de grupo de Gerador de Regras de Controle de Inicialização de Aplicativos é concluída.

Este cenário é recomendado para gerar listas de regras de permissão antes do primeiro início da política do Controle de dispositivos no modo da aplicação ativa de regras.

Antes de usar a política de Controle de Dispositivos na rede, certifique-se de que todos os computadores protegidos tenham acesso a uma pasta de rede compartilhada. Se a política da organização não prevê o uso de uma pasta de rede compartilhada na rede, recomenda-se começar a tarefa de Geradores de regras automatizadas para regras de controle do computador no grupo de computadores de teste ou em uma máquina modelo.

- Com base em um relatório sobre eventos de tarefa gerado no Kaspersky Security Center para a tarefa de Controle de dispositivos no modo **Somente estatísticas**.

  Segundo este cenário, o Kaspersky Embedded Systems Security 2.2 não restringe conexões de dispositivos de armazenamento em massa, mas registra informações sobre todas as conexões de dispositivos e registros de armazenamentos em massa em todos os computadores da rede durante a execução da tarefa de Controle de dispositivos no modo **Somente estatísticas**; as informações registradas podem ser encontradas na seção **Eventos** do Kaspersky Security Center. O Kaspersky Security Center gera a lista unificada de eventos de restrição e permissão de armazenamentos em massa, com base no log de tarefas.

  Você deve configurar o período de execução da tarefa de forma que todas as conexões de dispositivos de armazenamento em massa sejam realizadas durante o período estabelecido. Em seguida, conforme as regras são adicionadas à tarefa de Controle de dispositivos, você pode importar dados sobre as conexões de dispositivos do arquivo de relatório de evento salvo do Kaspersky Security Center (no formato TXT) e gerar regras de permissão de Controle de dispositivos para tais dispositivos com base nestes dados. O tipo dos eventos, no qual um log importado é baseado, não influencia no tipo de regras gerado; somente regras de permissão são geradas.

  Este cenário é recomendado para adicionar regras de permissão para um grande número de novos armazenamentos em massa, bem como gerar regras para dispositivos móveis confiáveis conectados por MTP.

- Com base nos dados do sistema sobre dispositivos de armazenamento em massa conectados (usando a opção Gerar regras com base nos dados do sistema nas configurações da política de Controle de Dispositivos).

  Segundo este cenário, o Kaspersky Embedded Systems Security 2.2 gera regras de permissão para armazenamentos em massa que já foram conectados ou estão atualmente conectados a um computador com o Kaspersky Security Center instalado.

  Este cenário é recomendado para gerar regras para um pequeno número de novos dispositivos de armazenamento em massa no qual você deseja confiar em todos os computadores na rede.

- Com base nos dados sobre os dispositivos atualmente conectados (usando **Gerar regras com base nos dispositivos conectados**).

  Neste cenário, o Kaspersky Embedded Systems Security 2.2 gera regras de permissão apenas para dispositivos conectados. É possível selecionar um ou mais dispositivos para os quais você deseja gerar regras de permissão.

O Kaspersky Embedded Systems Security 2.2 não tem acesso a dados do sistema sobre dispositivos móveis conectados via MTP. Você não pode gerar regras de permissão para dispositivos móveis confiáveis conectados via MTP usando cenários para o preenchimento da lista de regras na base de dados do sistema sobre todos os dispositivos conectados.

Geração de regras com base em dados do sistema sobre dispositivos externos conectados a computadores de rede

Você pode gerar regras (consulte a seção "Sobre a geração de regras de Controle de dispositivos para todos os computadores por meio do Kaspersky Security Center" na página 195) com base em dados do Windows sobre todos os armazenamentos em massa que já foram conectados ou que estejam conectados pelos três cenários:

- Usando a tarefa de grupo de Gerador de Regras de Controle de Dispositivos. Use este cenário durante o processo de geração de regras para considerar todos os armazenamentos em massa que já foram conectados e que são registrados pelos sistemas em todos os computadores de rede.
- Usando a opção **Gerar regras com base nos dados do sistema** nas configurações de política de Controle de dispositivos. Use este cenário durante o processo de geração de regras para considerar todos os armazenamentos em massa que já foram conectados e que são registrados pelo sistema do computador com o Console de Administração do Kaspersky Security Center instalado.
- Utilização de **Gerar regras com base nos dispositivos conectados** nas configurações da política de Controle de Dispositivos e a tarefa de Gerador de Regras de Controle de Dispositivos. Use este método se quiser considerar apenas os dados sobre dispositivos atualmente conectados ao computador protegido ao gerar as regras de permissão.

O Kaspersky Embedded Systems Security 2.2 não tem acesso a dados do sistema sobre dispositivos móveis conectados via MTP. Você não pode gerar regras de permissão para dispositivos móveis confiáveis conectados via MTP usando cenários para o preenchimento da lista de regras na base de dados do sistema sobre todos os dispositivos conectados.

Nesta seção

Criação de regras usando a tarefa de Gerador de Regras de Controle de Dispositivos

► *Para especificar regras de permissão de controle de dispositivos para um grupo de computadores usando a tarefa de Gerador de Regras de Controle de Dispositivos, execute as etapas a seguir.*

1. Na guia **Tarefas** no painel de controle do grupo de computadores que você está configurando, crie uma tarefa de grupo de Gerador de Regras de Controle de Dispositivos ou selecione uma tarefa existente.

2. Nas propriedades da tarefa de grupo de Gerador de Regras de Controle de Inicialização de Aplicativos criada ou no assistente de tarefa, especifique as seguintes configurações:
   - Na seção **Notificações**, defina as configurações para salvar o relatório de execução da tarefa.
   - Na seção **Configurações**, especifique as operações de tarefa após sua conclusão. Especifique o nome de arquivo onde as regras geradas serão exportadas.
   - Na janela **Programação**, defina as configurações da programação de inicialização da tarefa.
3. Na guia **Tarefas** no painel de controle do grupo de computadores sendo configurados, na lista de tarefas de grupo selecione o Gerador de Regras de Controle de Dispositivos que você criou e clique no botão **Iniciar** para iniciar a tarefa.

   Quando a tarefa é concluída, as listas de regras de permissão geradas automaticamente são salvas em uma pasta de rede compartilhada em arquivos XML.

   > Antes de usar a política de Controle de Dispositivos na rede, certifique-se de que todos os computadores protegidos tenham acesso a uma pasta de rede compartilhada. Se a política da organização não prevê o uso de uma pasta de rede compartilhada na rede, recomenda-se começar a tarefa de Geradores de regras automatizadas para regras de controle do computador no grupo de computadores de teste ou em uma máquina modelo.

4. Adicionar as listas geradas de regras de permissão à tarefa de Controle de dispositivos. Para fazer isso, nas propriedades da política que está sendo configurada, nas configurações de tarefa de Controle de dispositivos:

   a. Na guia **Geral**, clique no botão **Lista de regras**.

      A janela **Regras de Controle de dispositivos** é exibida.

   b. Clique no botão **Adicionar** e na lista exibida selecione **Importar regras do arquivo XML**.

   c. Selecione o princípio para adicionar as regras de permissão geradas automaticamente à lista de regras de Controle de dispositivos criadas anteriormente:
      - **Adicionar às regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
      - **Substituir as regras existentes** se deseja substituir as regras existentes com as importadas.
      - **Mesclar com as regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

   d. Na janela padrão do Microsoft Windows exibida, selecione arquivos XML criados após a conclusão da tarefa de grupo Gerador de Regras de Controle de Dispositivos.

   e. Clique em **OK** na janela Regras de Controle de dispositivos e na janela **Configurações de tarefa**.
5. Se você deseja aplicar as regras de controle de dispositivo geradas, selecione o modo de tarefa **Ativa** nas configurações de política de **Controle de dispositivos**.

Regras de permissão geradas automaticamente com base em dados do sistema em cada computador separado são aplicadas a todos os computadores de rede abrangidos pela política sendo configurada. Nestes computadores, o aplicativo permitirá a conexão somente daqueles dispositivos para os quais as regras de permissão foram criadas.

Criação de regras de permissão com base nos dados de sistema em uma política do Kaspersky Security Center

► *Para especificar regras de permissão usando a opção **Gerar regras com base nos dados do sistema** na política de Controle de dispositivos, siga estas etapas:*

1. Se necessário, conecte um novo armazenamento em massa no qual deseja confiar a um computador com o Console de Administração do Kaspersky Security Center instalado.
2. No Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciado**.
3. Expanda o grupo de administração cujas configurações de política você deseja configurar e selecione a guia **Políticas** no painel de detalhes.
4. Selecione **Propriedades** no menu de contexto da política que você deseja configurar.
5. A janela **Propriedades: <Nome da política>** é exibida.
6. Nas configurações da política, abra as configurações de tarefa de Controle de dispositivos e siga estas etapas:
   a. Na guia **Geral**, clique no botão **Lista de regras**.

      A janela **Regras de Controle de dispositivos** é exibida.
   b. Clique no botão **Adicionar** e no menu de contexto exibido selecione a opção **Gerar regras com base nos dados do sistema**.
   c. Selecione o princípio para adicionar as regras de permissão à lista de regras de Controle de dispositivos criadas anteriormente:
      - **Adicionar às regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
      - **Substituir as regras existentes** se deseja substituir as regras existentes com as importadas.
      - **Mesclar com as regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.
7. Clique em **OK** na janela **Regras de Controle de dispositivos** e na janela **Configurações de tarefa**.

A lista de regras na política de Controle de dispositivos será preenchida com novas regras geradas com base em dados do sistema do computador com o Console de Administração do Kaspersky Security Center instalado.

Geração de regras para dispositivos conectados

► *Para especificar regras de permissão usando a opção **Gerar regras com base nos dados do sistema** na política de Controle de dispositivos, siga estas etapas:*

1. No Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciado**.
2. Expanda o grupo de administração cujas configurações de política você deseja configurar e selecione a guia **Políticas** no painel de detalhes.
3. Selecione **Propriedades** no menu de contexto da política que você deseja configurar.
4. A janela **Propriedades: <Nome da política>** é exibida.
5. Na seção **Controle de Atividades Locais**, clique no botão **Configurações** na seção **Controle**

de dispositivos.

6. Na guia **Geral**, clique no botão **Lista de regras**.

   A janela **Regras de Controle de dispositivos** é exibida.

7. Clique no botão **Adicionar** e, no menu de contexto, selecione **Gerar regras com base nos dispositivos conectados**.

   A janela **Gerar regras com base nos dados do sistema** é exibida.

8. Na lista de dispositivos detectados conectados ao computador protegido, selecione os dispositivos para os quais você deseja gerar as regras de permissão.

9. Clique no botão **Adicionar regras para os dispositivos selecionados**.

10. Clique no botão **Salvar**, na janela **Controle de dispositivos**.

A lista de regras na política de Controle de dispositivos será preenchida com novas regras geradas com base em dados do sistema do computador com o Console de Administração do Kaspersky Security Center instalado.

Importação de regras do arquivo de relatório do Kaspersky Security Center sobre dispositivos restritos

Você pode importar dados sobre conexões de dispositivos restritos do relatório gerado no Kaspersky Security Center após a conclusão da tarefa de Controle de dispositivos no modo **Somente estatísticas** e usar estes dados para gerar uma lista de regras de permissão de Controle de dispositivos na política que está sendo configurada.

Ao gerar o relatório sobre eventos que ocorrem durante a tarefa de Controle de dispositivos, você poderá acompanhar os dispositivos cuja conexão é restringida.

Ao importar dados do relatório sobre dispositivos restringidos em configurações de política, certifique-se de que a lista sendo usada contenha somente dispositivos cuja conexão você deseja permitir.

► *Para especificar regras de permissão para a conexão de dispositivos para um grupo de computadores com base no relatório do Kaspersky Security Center sobre dispositivos restringidos, siga as etapas a seguir:*

1. Nas propriedades de política nas configurações da tarefa de Controle de dispositivos, selecione o modo **Somente estatísticas**.
2. Nas propriedades de política na seção **Eventos**, certifique-se de que:
   - A guia **Eventos críticos** do evento *Armazenamento em massa restrito* mostra um tempo de armazenamento de evento que excede o tempo planejado de operação da tarefa no modo **Somente estatísticas** (o valor padrão é 30 dias).
   - A guia **Aviso** do evento *Somente estatísticas: armazenamento em massa não confiável detectado* mostra um tempo de armazenamento de evento que excede o tempo planejado de operação da tarefa no modo **Somente estatísticas** (o valor padrão é 30 dias).

   Quando o período especificado na coluna **Tempo de armazenamento** é excedido, as informações sobre eventos registrados são excluídas e não são refletidas no arquivo de relatório. Antes de executar a tarefa de Controle de dispositivos no modo **Somente estatísticas**, certifique-se de que o tempo de execução da tarefa não exceda o tempo de armazenamento configurado para os eventos especificados.
3. Após a tarefa ter sido concluída, exporte os eventos registrados para um arquivo TXT. Para fazer isso, expanda o nó **Logs e notificações** e no nó filho, **Eventos**, crie uma seleção de eventos com base no critério *Negado* para visualizar os dispositivos cujas conexões serão restringidas pela tarefa de Controle de dispositivos. No painel de detalhes da seleção, clique na lista **Exportar eventos** para arquivo para salvar o relatório de inicializações de aplicativos bloqueadas em um arquivo TXT.

   Antes de importar e aplicar o relatório gerado em uma política, certifique-se de que o relatório contenha somente dados sobre os dispositivos cuja conexão você deseja permitir.
4. Importar dados sobre conexões de dispositivos restringidas na política de Controle de dispositivos. Para fazer isso, nas propriedades da política que está sendo configurada, nas configurações de tarefa de Controle de dispositivos, siga as etapas a seguir:
   a. Na guia **Geral**, clique no botão **Lista de regras**.

      A janela **Regras de Controle de dispositivos** é exibida.

   b. Clique no botão **Adicionar** e, no menu de contexto do botão, selecione **Importar dados de dispositivos bloqueados do relatório do Kaspersky Security Center**.

c. Selecione o princípio para adicionar regras da lista criada com base no relatório do Kaspersky Security Center à lista de regras de Controle de dispositivos previamente configuradas:

   - **Adicionar às regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
   - **Substituir as regras existentes** se deseja substituir as regras existentes com as importadas.
   - **Mesclar com as regras existentes** se deseja adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

d. Na janela padrão do Microsoft Windows exibida, selecione o arquivo TXT ao qual os eventos do relatório sobre dispositivos restringidos foram exportados.

e. Clique em **OK** na janela **Regras de Controle de dispositivos** e na janela **Configurações de tarefa**.

As regras criadas com base no relatório do Kaspersky Security Center sobre dispositivos restringidos são adicionadas à lista de regras de Controle de dispositivos.

Controle de atividade de rede

Esta seção contém informações sobre a tarefa Gerenciamento de Firewall.

Gerenciamento de Firewall

Esta seção contém informações sobre a tarefa Gerenciamento de Firewall e como configurá-la.

Nesta seção

Sobre a tarefa de Gerenciamento de Firewall

O Kaspersky Embedded Systems Security 2.2 fornece uma solução confiável e ergonômica para proteger conexões de rede usando a tarefa de Gerenciamento de Firewall.

A tarefa de Gerenciamento de Firewall não executa a filtragem de tráfego de rede independente, mas permite que você gerencie o Firewall do Windows por meio da interface gráfica do Kaspersky Embedded Systems Security 2.2. Durante a tarefa de Gerenciamento de Firewall, o Kaspersky Embedded Systems Security 2.2 assume o gerenciamento das configurações e políticas do Firewall do sistema operacional e bloqueia qualquer possibilidade de configuração externa do Firewall.

Durante a instalação do aplicativo, o componente de Gerenciamento de Firewall lê e copia o status do Firewall do Windows e todas as regras especificadas. Depois disso, o conjunto de regras e os parâmetros da regra podem apenas ser alterados, e o Firewall pode apenas ser ativado ou desativado no Kaspersky Embedded Systems Security 2.2.

Se o Firewall do Windows for desativado durante a instalação do Kaspersky Embedded Systems Security 2.2, a tarefa de Gerenciamento de Firewall não será executada após a conclusão da instalação. Se o Firewall do Windows for ativado durante a instalação do aplicativo, a tarefa de Gerenciamento de Firewall será executada após a instalação ser concluída, bloqueando todas as conexões de rede que não são permitidas pelas regras especificadas.

O componente de Gerenciamento de Firewall não é instalado por padrão, já que não está incluído no conjunto de componentes para a Instalação recomendada.

A tarefa de Gerenciamento de Firewall impõe o bloqueio de todas as conexões de entrada e de saída não permitidas pelas regras especificadas da tarefa.

A tarefa pesquisa o Firewall do Windows regularmente e monitora o seu status. Por padrão, o intervalo de pesquisa é definido como 1 minuto e não pode ser alterado. Se durante a pesquisa, o Kaspersky Embedded Systems Security 2.2 detectar ausência de correspondência entre as configurações do Firewall do Windows e as da tarefa de Gerenciamento de Firewall, o aplicativo aplicará de maneira forçada as configurações da tarefa ao Firewall do sistema operacional.

Com a pesquisa minuto a minuto do Firewall do Windows, o Kaspersky Embedded Systems Security 2.2 monitorará o seguinte:

- O status de operação do Firewall do Windows.
- O status de regras adicionadas após a instalação do Kaspersky Embedded Systems Security 2.2 por outros aplicativos ou ferramentas (por exemplo, a adição de uma nova regra de aplicativo para uma porta/aplicativo usando o wf.msc).

Ao aplicar as novas regras ao Firewall do Windows, o Kaspersky Embedded Systems Security 2.2 cria um conjunto de regra do Kaspersky Security Group no snap-in do **Firewall do Windows**. Esse conjunto de regras une todas as regras criadas pelo Kaspersky Embedded Systems Security 2.2 usando a tarefa de Gerenciamento de Firewall. As regras no Kaspersky Security Group não são monitoradas pelo aplicativo durante a pesquisa a cada minuto e não são automaticamente sincronizadas com a lista de regras especificadas nas configurações da tarefa de Gerenciamento de Firewall.

► *Para atualizar manualmente as regras do Kaspersky Security Group,*

Reinicie a tarefa de Gerenciamento de Firewall do Kaspersky Embedded Systems Security 2.2.

Também é possível editar as regras do Kaspersky Security Group manualmente usando o snap-in do **Firewall do Windows**.

Se o Firewall do Windows for gerenciado pela política de grupo do Kaspersky Security Center, a tarefa de Gerenciamento de Firewall não poderá ser iniciada.

Sobre as Regras de Firewall

A tarefa de Gerenciamento de Firewall controla a filtragem do tráfego de entrada e de saída da rede usando regras de permissão aplicadas de maneira forçada no Firewall do Windows durante a execução da tarefa.

A primeira vez que a tarefa é iniciada, o Kaspersky Embedded Systems Security 2.2 lê e copia todas as regras de tráfego de rede recebido especificadas nas configurações do Firewall do Windows nas configurações da tarefa de Gerenciamento de Firewall. Em seguida, o aplicativo funciona de acordo com as seguintes regras:

- Se uma nova regra for criada nas configurações do Firewall do Windows (manual ou automaticamente durante uma nova instalação do aplicativo), o Kaspersky Embedded Systems Security 2.2 excluirá a regra;
- Se uma regra existente for excluída das configurações do Firewall do Windows, o Kaspersky Embedded Systems Security 2.2 restaurará a regra;
- Se os parâmetros de uma regra existente forem alterados nas configurações do Firewall do Windows, o Kaspersky Embedded Systems Security 2.2 reverterá as alterações;
- Se uma nova regra for criada nas configurações da Gerenciamento de Firewall, o Kaspersky Embedded

Systems Security 2.2 aplicará de maneira forçada essa regra ao Firewall do Windows;

- Se uma regra existente for excluída das configurações de Gerenciamento de Firewall, o Kaspersky Embedded Systems Security 2.2 será forçado a excluir a regra das configurações do Firewall do Windows.

O Kaspersky Embedded Systems Security 2.2 não funciona com regras de bloqueio ou regras de controle do tráfego de saída de rede. Após o início da tarefa de Gerenciamento de Firewall, o Kaspersky Embedded Systems Security 2.2 excluirá todas essas regras das configurações do Firewall do Windows.

É possível definir, excluir e editar as regras de filtragem para o tráfego de rede de entrada.

Não é possível especificar uma nova regra para controlar o tráfego de rede de saída nas configurações da tarefa de Gerenciamento de Firewall. Todas as regras de Firewall especificadas no Kaspersky Embedded Systems Security 2.2 controlam apenas o tráfego de rede de entrada.

É possível gerenciar os seguintes tipos de regras de Firewall:

- Regras do aplicativo.
- Regras da porta.

Regras do aplicativo

Este tipo de regra permite conexões direcionadas de rede para aplicativos especificados. O critério de acionamento para estas regras baseia-se em um caminho para um arquivo executável.

É possível gerenciar regras do aplicativo:

- Adicionar novas regras.
- Remover regras existentes.
- Ativar ou desativar regras especificadas.
- Editar os parâmetros das regras especificadas: especifique o nome da regra, caminho até o arquivo executável e escopo de utilização da regra.

Regras da porta

Este tipo de regra permite conexões de rede para portas e protocolos (TCP/UDP) especificados. Os critérios de acionamento para estas regras baseiam-se no número da porta e tipo de protocolo.

É possível gerenciar regras de portas:

- Adicionar novas regras.
- Remover regras existentes.
- Ativar ou desativar regras especificadas.
- Editar os parâmetros das regras especificadas: defina o nome da regra, número da porta, tipo de protocolo e escopo para o aplicativo da regra.

As regras de porta implicam um escopo mais amplo do que as de aplicativo. Ao permitir conexões com base nas regras de porta, você reduz o nível de segurança do computador protegido.

Como ativar e desativar as regras de Firewall

► *Para ativar ou desativar uma regra existente para a filtragem do tráfego de entrada de rede, execute as seguintes ações:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

     Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Controle de atividade de rede**, clique no botão **Configurações** no bloco **Gerenciamento de Firewall.**
4. Clique no botão **Lista de regras** na janela que se abre.

   A janela **Lista de regras** é exibida.
5. Dependendo do tipo da regra cujo status você deseja modificar, selecione **Aplicativos** ou **Portas**.
6. Na lista de regras, selecione a regra cujo status você deseja modificar e execute uma das seguintes ações:
   - Se você quiser ativar uma regra desativada, marque a caixa de seleção à esquerda do nome da regra.

     A regra selecionada será ativada.
   - Se você quiser desativar uma regra ativada, desmarque a caixa de seleção à esquerda do nome da regra.

     A regra selecionada será desativada.
7. Clique em **Salvar** na janela **Lista de regras**.

As configurações da tarefa especificadas serão salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Adição de regras de Firewall manualmente

É possível apenas adicionar e editar regras para aplicativos e portas. Não é possível adicionar ou editar regras de grupos existentes.

► *Para adicionar ou editar uma regra existente para a filtragem de tráfego de entrada de rede, faça o seguinte:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
    - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
    - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

    > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Controle de atividade de rede**, clique no botão **Configurações** no bloco **Gerenciamento de Firewall**.
4. Clique no botão **Lista de regras** na janela que se abre.

    A janela **Lista de regras** é exibida.
5. Dependendo do tipo de regra que você deseja adicionar, selecione a guia **Aplicativos** ou **Portas** e execute uma das seguintes ações:
    - Para editar uma regra existente, selecione a regra que deseja editar na lista de regras e clique em **Editar**.
    - Para adicionar uma nova regra, clique em **Adicionar**.

      Dependendo do tipo de regra que estiver sendo configurada, a janela **Regra da porta** ou **Regra de aplicativo** é exibida.
6. Na janela exibida, execute as seguintes operações:
    - Se você estiver trabalhando com uma regra de aplicativo, faça o seguinte:
        a. Digite o **Nome da regra** editada.
        b. Especifique o **Caminho do aplicativo** para o arquivo executável do aplicativo para o qual você está permitindo uma conexão modificando esta regra.

           É possível configurar o caminho manualmente ou usando o botão **Procurar**.
        c. No campo **Escopo de aplicação da regra**, especifique os endereços de rede aos quais a regra modificada será aplicada.

           > Você pode usar apenas endereços IP IPv4.
    - Se você estiver trabalhando com uma regra de porta, faça o seguinte:
        a. Digite o **Nome da regra** editada.

b. Especifique o **Número da porta** para o qual o aplicativo permitirá conexões.

c. Selecione o tipo de protocolo (TCP/UDP) para o qual o aplicativo permitirá conexões.

d. No campo **Escopo de aplicação da regra**, especifique os endereços de rede aos quais a regra modificada será aplicada.

> Você pode usar apenas endereços IP IPv4.

7. Clique em **OK** na janela **Regra de aplicativo** ou **Regra da porta**.
8. Clique em **Salvar** na janela **Regras de Firewall**.

As configurações da tarefa especificadas serão salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Exclusão de regras de Firewall

> Só é possível excluir regras de aplicativos e de porta. Não é possível excluir regras de grupo existentes.

► *Para excluir uma regra existente para a filtragem do tráfego de entrada de rede, execute as seguintes ações:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Controle de atividade de rede**, clique no botão **Configurações** no bloco **Gerenciamento de Firewall.**
4. Clique no botão **Lista de regras** na janela que se abre.

   A janela **Lista de regras** é exibida.
5. Dependendo do tipo da regra cujo status você deseja modificar, selecione a guia **Aplicativos** ou **Portas**.
6. Na lista de regras, selecione a regra que você deseja excluir.
7. Clique no botão **Remover**.

   A regra selecionada é excluída.
8. Clique em **Salvar** na janela **Regras de Firewall**.

As configurações da tarefa de Gerenciamento de Firewall especificadas são salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Inspeção do sistema

Esta seção contém informações sobre a tarefa Monitor de Integridade de Arquivos e recursos para inspecionar o log do sistema operacional.

Neste capítulo

Monitor de Integridade de Arquivos

Esta seção contém informações sobre a inicialização e a configuração da tarefa de Monitor de Integridade de Arquivos.

Nesta seção

Sobre a tarefa Monitor de Integridade de Arquivos

A tarefa Monitor de Integridade de Arquivos foi projetada para rastrear ações realizadas com os arquivos e as pastas especificados nos escopos de monitoramento definidos nas configurações da tarefa. É possível usar a tarefa para detectar alterações no arquivo que possam indicar uma violação de segurança no computador protegido. Também é possível configurar que as alterações no arquivo sejam rastreadas durante períodos em que o monitoramento é interrompido.

Uma *interrupção do monitoramento* ocorre quando o escopo do monitoramento fica temporariamente fora do escopo da tarefa, por exemplo, se a tarefa for interrompida ou se um dispositivo protegido não estiver fisicamente presente em um computador protegido. O Kaspersky Embedded Systems Security 2.2 informa operações de arquivos detectadas no escopo de monitoramento assim que o dispositivo de armazenamento em massa é reconectado.

> Se as tarefas deixarem de ser executadas no escopo de monitoramento especificado devido a uma reinstalação do componente do Monitor de Integridade de Arquivos, isso não constituirá uma interrupção do monitoramento. Neste caso, a tarefa de Monitor de Integridade de Arquivos não é executada.

Requisitos no ambiente

Para iniciar a tarefa Monitor de Integridade de Arquivos, as seguintes condições devem ser satisfeitas:

- Um dispositivo de armazenamento compatível com os sistemas ReFS e NTFS deve ser instalado no computador protegido.
- O USN Journal do Windows deve estar ativo. O componente solicita ao Journal para receber informações sobre as operações do arquivo.

> Se você ativar o USN Journal após uma regra ter sido criada para um volume e a tarefa de Monitor de Integridade de Arquivos tiver sido iniciada, a tarefa deverá ser reiniciada. Senão, a regra não será aplicada durante o monitoramento.

Escopos de monitoramento excluídos

Você pode criar exclusões do escopo de monitoramento (consulte a seção "Configuração de regras de monitoramento" na página 215). As exclusões são especificadas para cada regra separada e funcionam apenas para o escopo de monitoramento indicado. É possível especificar um número ilimitado de exclusões para cada regra.

> As exclusões têm uma prioridade mais alta do que o escopo de monitoramento e não são monitoradas pela tarefa, mesmo se uma pasta ou arquivo indicado estiver no escopo. Se as configurações para uma das regras especificarem um escopo de monitoramento em um nível inferior do que a pasta especificada nas exclusões, este não será considerado quando a tarefa for executada.

Para especificar exclusões, você pode usar as mesmas máscaras que as utilizadas para especificar escopos de monitoramento.

Sobre regras de monitoramento de operações de arquivos

O Monitor de Integridade de Arquivos é executado com base nas regras de monitoramento de operações de arquivos. É possível usar os critérios para acionamento de regras para configurar as condições que acionam a tarefa e ajustar o nível de importância dos eventos para operações de arquivo detectadas e registradas no log de tarefas.

Uma regra de monitoramento de operações de arquivos é especificada para cada escopo de monitoramento.

É possível configurar os seguintes critérios para acionamento de regras:

- Usuários confiáveis.
- Marcadores de operação de arquivo.

Usuários confiáveis

Por padrão, o aplicativo trata todas as ações de usuário como potenciais violações de segurança. A lista de usuários confiáveis está vazia. É possível configurar o nível de importância de evento criando uma lista de usuários confiáveis nas configurações de regra de monitoramento de operações de arquivo.

Usuário não confiável – qualquer usuário não indicado na lista de usuário confiável nas configurações da regra de escopo de monitoramento. Se o Kaspersky Embedded Systems Security 2.2 detectar uma operação de arquivo realizada por um usuário não confiável, a tarefa Monitor de Integridade de Arquivos registrará um Evento crítico no log de tarefas.

Usuário confiável – um usuário ou grupo de usuários autorizados a realizar operações de arquivo no escopo de monitoramento especificado. Se o Kaspersky Embedded Systems Security 2.2 detectar operações de arquivo realizadas por um usuário confiável, a tarefa Monitor de Integridade de Arquivos registrará um evento informativo no log de tarefas.

O Kaspersky Embedded Systems Security 2.2 não é capaz de determinar os usuários que iniciam operações durante os períodos de interrupção do monitoramento. Neste caso, o status do usuário é determinado como desconhecido.

Usuário desconhecido – Este status é atribuído a um usuário se o Kaspersky Embedded Systems Security 2.2 não puder receber informações sobre um usuário devido a uma interrupção da tarefa ou uma falha no driver de sincronização de dados ou USN Journal. Se o Kaspersky Embedded Systems Security 2.2 detectar uma operação de arquivo realizada por um usuário desconhecido, a tarefa Monitor de Integridade de Arquivos registrará um evento de *Aviso* no log de tarefas.

Marcadores de operação de arquivo

Quando a tarefa Monitor de Integridade de Arquivos for executada, o Kaspersky Embedded Systems Security 2.2 usará os marcadores de operação de arquivo para determinar que uma ação foi realizada em um arquivo.

Um marcador de operação de arquivo é um descritor exclusivo que pode caracterizar uma operação de arquivo.

Cada operação de arquivo pode ser uma ação única ou uma cadeia de ações com arquivos. Cada ação dessa espécie é comparada a um marcador de operação de arquivo. Se o marcador especificado como um critério para acionamento de regras for detectado em uma cadeia de operação de arquivo, o aplicativo registrará um evento indicando que a determinada operação de arquivo foi realizada.

O nível de importância dos eventos registrados em log não depende dos marcadores de operação de arquivo selecionados ou do número de eventos.

Por padrão, o Kaspersky Embedded Systems Security 2.2 considera todos os marcadores de operação de arquivo disponíveis. É possível selecionar marcadores de operação de arquivo manualmente nas configurações de regra da tarefa.

Tabela 36. Marcadores de operação de arquivo

ID de operação de arquivo	Marcador de operação de arquivo	Sistemas de arquivos compatíveis
BASIC_INFO_CHANGE	Os atributos ou marcadores de tempo de um arquivo ou pasta foram alterados	NTFS, ReFS
COMPRESSION_CHANGE	A compactação de um arquivo ou pasta foi alterada	NTFS, ReFS
DATA_EXTEND	O tamanho de um arquivo ou pasta foi aumentado	NTFS, ReFS
DATA_OVERWRITE	Os dados em um arquivo ou pasta foram substituídos	NTFS, ReFS
DATA_TRUNCATION	Arquivo ou pasta truncados	NTFS, ReFS
EA_CHANGE	Os atributos do arquivo ou pasta estendidos foram alterados	Somente NTFS
ENCRYPTION_CHANGE	O status de criptografia de um arquivo ou pasta foi alterado	NTFS, ReFS
FILE_CREATE	Arquivo ou pasta criados pela primeira vez	NTFS, ReFS

ID de operação de arquivo	Marcador de operação de arquivo	Sistemas de arquivos compatíveis
FILE_DELETE	O arquivo ou a pasta foi permanentemente excluído usando a combinação SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	Conexão física criada ou excluída para o arquivo ou pasta	Somente NTFS
INDEXABLE_CHANGE	O status de indexação de um arquivo ou pasta foi alterado	NTFS, ReFS
INTEGRITY_CHANGE	O atributo de integridade foi alterado para um fluxo de arquivo nomeado	Somente ReFS
NAMED_DATA_EXTEND	O tamanho de um fluxo de arquivo nomeado foi aumentado	NTFS, ReFS
NAMED_DATA_OVERWRITE	Fluxo do arquivo nomeado substituído	NTFS, ReFS
NAMED_DATA_TRUNCATION	Fluxo do arquivo nomeado truncado	NTFS, ReFS
OBJECT_ID_CHANGE	Identificador de arquivo ou pasta alterado	NTFS, ReFS
RENAME_NEW_NAME	Novo nome atribuído ao arquivo ou à pasta	NTFS, ReFS
REPARSE_POINT_CHANGE	O novo ponto de reanálise criado ou existente alterado para um arquivo ou pasta	NTFS, ReFS
SECURITY_CHANGE	Direitos de acesso de arquivo ou pasta alterados	NTFS, ReFS
STREAM_CHANGE	Nova fluxo de arquivo nomeado criado ou existente alterado	NTFS, ReFS
TRANSACTED_CHANGE	Fluxo de arquivo nomeado alterado pela transação TxF	Somente ReFS

Configuração da tarefa Monitor de Integridade de Arquivos

É possível alterar as configurações padrão da tarefa de Monitor de Integridade de Arquivos (consulte a tabela abaixo).

Tabela 37. Configurações padrão da tarefa de Monitor de Integridade de Arquivos

Configuração	Valor padrão	Descrição
Escopo de monitoramento	Não configurado	É possível especificar as pastas e os arquivos para os quais as ações serão monitoradas. Os eventos de monitoramento serão gerados para as pastas e os arquivos no escopo de monitoramento especificado.
Lista de usuários confiáveis	Não configurado	É possível especificar usuários e/ou grupos de usuários cujas ações nos diretórios especificados serão tratadas como seguras pelo componente.

Configuração	Valor padrão	Descrição
Monitorar operações de arquivo quando a tarefa não for executada	Usada	É possível ativar ou desativar o registro de operações de arquivo em log executadas nos escopos de monitoramento indicados durante os períodos em que a tarefa não está sendo executada.
Considere escopo de monitoramento excluído	Não aplicado	É possível verificar o uso de exclusões das pastas onde as operações de arquivo não precisam ser monitoradas. Quando a tarefa Monitor de Integridade de Arquivos for executada, o Kaspersky Embedded Systems Security 2.2 ignorará os escopos de monitoramento especificados como exclusões.
Cálculo da soma de verificação	Não aplicado	É possível configurar o cálculo da soma de verificação de arquivo depois que as alterações no arquivo forem feitas.
Considerar marcadores de operação de arquivo	Todos os marcadores de operação de arquivo disponíveis serão considerados	É possível especificar o conjunto de marcadores de operação de arquivo. Se uma operação de arquivo executada em um escopo de monitoramento for caracterizada por um ou mais marcadores especificados, ao Kaspersky Embedded Systems Security 2.2 gerará um evento de auditoria.
Programação de inicialização de tarefa	A primeira execução não está programada	Você pode definir as configurações da inicialização programada da tarefa.

► *Para definir as configurações gerais da tarefa Monitor de Integridade de Arquivos, implemente as seguintes etapas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Inspeção do sistema**, na seção **Monitor de Integridade de Arquivos**, clique no botão **Configurações**.

   A janela **Monitor de Integridade de Arquivos** é aberta.

4. Na guia **Definição de operação de monitoramento de arquivo** na janela exibida, defina as configurações de escopo de monitoramento:
   a. Desmarque ou selecione a caixa de seleção **Informações de log sobre operações de arquivo que aparecem durante o período de interrupção do monitoramento**.

      A caixa de seleção ativa ou desativa o monitoramento das operações de arquivo especificadas nas configurações da tarefa Monitor de Integridade de Arquivos quando a tarefa não estiver sendo executada por alguma razão (remoção de um disco rígido, tarefa interrompida pelo usuário, erro de software).

      Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 registrará eventos em todos os escopos de monitoramento quando a tarefa Monitor de Integridade de Arquivos não estiver sendo executada.

      Se a caixa de seleção for desmarcada, o aplicativo não registrará em log operações de arquivo em escopos de monitoramento quando a tarefa não estiver sendo executada.

      A caixa de seleção é selecionada por padrão.
   b. Adicione os escopos de monitoramento (consulte a seção "Configuração de regras de monitoramento" na página 215) a serem monitorados pela tarefa.
5. Na guia **Gerenciamento da tarefa**, inicie a tarefa baseada em uma programação (consulte a seção "Gerenciando programações de tarefas" na página 121).
6. Clique em **OK** para salvar as alterações.

Configuração de regras de monitoramento

Por padrão, um escopo de monitoramento não é especificado e a tarefa não monitora as operações de arquivo em nenhum diretório.

► *Para adicionar um escopo de monitoramento, execute estas etapas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Inspeção do sistema**, na seção **Monitor de Integridade de Arquivos**, clique no botão **Configurações**.

   A janela **Propriedades: Monitor de Integridade de Arquivos** é aberta.

4. Na seção **Escopo de monitoramento**, clique no botão **Adicionar**.

   A janela **Escopo de monitoramento** é aberta.

5. Adicione um escopo de monitoramento de uma das seguintes formas:

   - Se quiser selecionar pastas através da caixa de diálogo padrão do Microsoft Windows:

     a. Clique no botão **Procurar**.

        A janela padrão Procurar Pasta do Microsoft Windows é aberta.

     b. Na janela exibida, selecione a pasta para a qual deseja monitorar operações e clique no botão **OK**.

   - Se quiser especificar um escopo de monitoramento manualmente, adicione um caminho usando uma máscara com suporte:

     - <*.ext> - todos os arquivos com a extensão <ext>, independentemente da sua localização;
     - <*\nome.ext> - todos os arquivos com o nome <nome> e a extensão <ext>, independentemente da sua localização;
     - <\dir*> - todos os arquivos no diretório <\dir>;
     - <\dir*\nome.ext> - todos os arquivos com o nome <nome> e a extensão <ext> no diretório <\dir> e todos dos seus subdiretórios.

   > Ao especificar um escopo de monitoramento manualmente, certifique-se de que o caminho esteja no seguinte formato: <letra do volume>: \<máscara>. Se a letra do volume estiver faltando, o Kaspersky Embedded Systems Security 2.2 não adicionará o escopo de monitoramento especificado.

6. Na guia **Usuários confiáveis**, clique no botão **Adicionar**.

   A janela **Selecionar usuários ou grupos** padrão do Microsoft Windows é exibida.

7. Selecione os usuários ou grupos de usuários para quem as operações de arquivo serão permitidas no escopo de monitoramento selecionado e clique no botão **OK**.

   > Por padrão, o Kaspersky Embedded Systems Security 2.2 trata todos os usuários que não estejam na lista de usuários confiáveis como não confiáveis (consulte a seção "Sobre regras de monitoramento de operações de arquivos" na página 211), e gera eventos críticos para eles.

8. Selecione a guia **Marcadores de operação do arquivo**.

9. Se necessário, realize as ações a seguir para selecionar um número de marcadores:

   a. Selecione a opção **Detectar operações de arquivo com base nos seguintes marcadores**.

   b. Na lista de operações de arquivos disponíveis (consulte a seção "Sobre regras de monitoramento de operações de arquivos" na página 211), selecione as caixas ao lado das operações que deseja monitorar.

   > Por padrão, o Kaspersky Embedded Systems Security 2.2 detecta todos os marcadores de operação de arquivos, a opção **Detectar operações de arquivo com base em todos os marcadores reconhecíveis** está marcada.

10. Se quiser que o Kaspersky Embedded Systems Security 2.2 calcule a soma de verificação de arquivos após a operação ser realizada, faça o seguinte:
    a. Na seção **Cálculo da soma de verificação**, marque a caixa de seleção **Calcule a soma de verificação para uma versão final de arquivo, depois que o arquivo for alterado, se possível**.

        Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 calculará a soma de verificação do arquivo modificado, no qual a operação de arquivo com pelo menos um marcador selecionado tenha sido detectada.

        Se a operação de arquivo for detectada por um número de marcadores, apenas a soma de verificação do arquivo final após todas as modificações será calculada.

        Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 não calculará a soma de verificação para os arquivos modificados.

        Nenhum cálculo da soma de verificação será realizado nos casos a seguir:

        - Se o arquivo ficar indisponível (por exemplo, devido à modificação de permissões de acesso).
        - Se a operação de arquivo for detectada no arquivo que foi removido posteriormente.

        Esta caixa é desmarcada por padrão.
    b. Na lista suspensa **Calcule a soma de verificação usando o algoritmo**, selecione uma das opções:
        - **Hash MD5**
        - **Hash SHA256**
11. Se você não quiser monitorar todas as operações de arquivo na lista de operações de arquivo disponíveis (consulte a seção “Sobre regras de monitoramento de operações de arquivos” na página 211), marque as caixas de seleção ao lado das operações que deseja monitorar.
12. Se necessário, adicione escopos de monitoramento realizando as seguintes etapas:
    a. Selecione a guia **Exclusões**.
    b. Marque a caixa de seleção **Considere o escopo de monitoramento excluído**.

        A caixa de seleção desativa o uso de exclusões das pastas onde as operações de arquivo não precisam ser monitoradas.

        Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 ignorará os escopos de monitoramento especificados na lista de exclusões quando a tarefa Monitor de Integridade de Arquivos for executada.

        Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security 2.2 registrará eventos para todos os escopos de monitoramento especificados.

        Por padrão, a caixa de seleção está desmarcada e a lista de exclusão, vazia.
    c. Clique no botão **Adicionar**.

        A janela **Selecionar pasta para adicionar** é exibida.
    d. Na janela exibida, especifique a pasta que deseja excluir do escopo de monitoramento.
    e. Clique em **OK**.

        A pasta especificada é adicionada à lista de escopos excluídos.
13. Clique em **OK** na janela **Escopo de monitoramento**.

    As configurações de regra especificada serão aplicadas ao escopo de monitoramento selecionado da tarefa de Monitor de integridade de arquivo.

Inspeção do Log

Esta seção contém informações sobre a tarefa de Inspeção do Log e definição de configurações de tarefa.

Nesta seção

Sobre a tarefa de Inspeção do Log

Quando a tarefa de Inspeção do Log é executada, o Kaspersky Embedded Systems Security 2.2, monitora a integridade do ambiente protegido com base nos resultados de uma inspeção dos Logs de Eventos do Windows. O aplicativo notifica o administrador quando detecta um comportamento anormal no sistema, que pode ser uma indicação de tentativas de ataques cibernéticos.

O Kaspersky Embedded Systems Security 2.2 considera os logs de eventos do Windows e identifica violações com base nas regras especificadas por um usuário ou pelas configurações do Analisador Heurístico, utilizado pela tarefa para inspecionar logs.

Regras predefinidas e análise heurística

É possível utilizar a tarefa de Inspeção do Log para monitorar o estado do sistema protegido com base na heurística existente. O analisador heurístico identifica atividade anormal no computador protegido, o que pode ser uma evidência de tentativa de ataque. Modelos para identificar comportamento anormal estão incluídos nas regras disponíveis nas configurações de regras predefinidas.

Sete regras estão incluídas na lista de regras da tarefa de Inspeção do Log. Você pode ativar ou desativar o uso de qualquer uma dessas regras. Não é possível eliminar as regras existentes ou criar novas regras.

É possível configurar critérios de acionamento de regras que monitoram eventos para as seguintes operações:

- Detecção de ataque de força bruta de senha
- Detecção de login na rede

Também é possível configurar exclusões nas configurações da tarefa. O analisador heurístico não é ativado quando um login é realizado por um usuário confiável ou a partir de um endereço IP confiável.

> O Kaspersky Embedded Systems Security 2.2 não usa a heurística para inspecionar os logs do Windows se o Analisador Heurístico não for usado pela tarefa. Por padrão, o analisador heurístico fica ativo.

Quando as regras são aplicadas, o aplicativo registra um *Evento crítico* no log de tarefas de Inspeção do Log.

Regras personalizadas para a tarefa de Inspeção do Log

Você pode usar as configurações de regra de tarefa para especificar e alterar os critérios para as regras de acionamento após a detecção de eventos selecionados no log especificado do Windows. Por padrão, a lista das regras da tarefa de Inspeção do Log contém quatro regras. Você pode ativar e desativar o uso dessas regras, removê-las e editar suas configurações.

Você pode configurar os seguintes critérios para acionamento de regras para cada uma delas:

- Lista de identificadores no Log de Eventos do Windows.

  A regra é acionada quando um novo registro é criado no Log de Eventos do Windows, se as propriedades de eventos incluírem um identificador de evento especificado para a regra. Também é possível adicionar e remover identificadores para cada regra especificada.

- Fonte de evento.

  Para cada regra, é possível definir um sublog do Log de Eventos do Windows. O aplicativo procurará registros com os identificadores de evento especificados apenas nesse sublog. Você pode selecionar um dos sublogs padrão (Aplicativo, Segurança ou Sistema), ou especificar um sublog personalizado digitando o nome no campo de seleção de fonte.

  > O aplicativo não verifica se o sublog especificado realmente existe no Log de Eventos do Windows.

Quando a regra é acionada, o Kaspersky Embedded Systems Security 2.2 registra um Evento crítico no log de tarefas de Inspeção do Log.

Por padrão, a tarefa de Inspeção do Log não aplica regras personalizadas.

> Antes de iniciar a tarefa de Inspeção do Log certifique-se de que a política de auditoria do sistema esteja configurada corretamente. Consulte o artigo da Microsoft https://technet.microsoft.com/en-us/library/cc952128.aspx para detalhes.

Configuração de regras de tarefa predefinidas

► *Realize as seguintes ações para configurar regras predefinidas para a tarefa de Inspeção do Log:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
3. Na seção **Inspeção do sistema**, clique no botão **Configurações** no bloco **Inspeção do Log**.

   A janela **Configurações de Inspeção do Log** é exibida.
4. Selecione a guia **Regras predefinidas**.

5. Marque ou desmarque a caixa de seleção **Aplicar regras predefinidas para inspeção do log**.

    Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security 2.2 aplicará o analisador heurístico para detectar atividade anormal no computador protegido.

    Se esta caixa de seleção for desmarcada, o analisador heurístico não será executado e o Kaspersky Embedded Systems Security 2.2 aplicará regras predefinidas ou personalizadas para detectar atividade anormal.

    A caixa de seleção é selecionada por padrão.

    > Para que a tarefa seja executada, pelo menos uma regra de inspeção do log deve ser selecionada.

6. Selecione as regras que deseja aplicar, na lista de regras predefinidas:
    - Existem padrões de um possível ataque de força bruta no sistema.
    - Existem padrões de uma possível violação no Log de Eventos do Windows.
    - Ações atípicas detectadas em nome de um novo serviço instalado.
    - Detectado login atípico que usa credenciais explícitas.
    - Existem padrões de um possível ataque PAC se passando por Kerberos (MS14-068) no sistema.
    - Ações atípicas detectadas, direcionadas a Administradores do grupo integrado privilegiado.
    - Foi detectada uma atividade atípica durante uma sessão de login na rede.
7. Para configurar as regras selecionadas, clique no botão **Configurações avançadas**.

    A janela **Inspeção do Log** é exibida.
8. Na seção **Detecção de ataque de força bruta**, defina o número de tentativas e um período quando essas tentativas ocorreram, que serão considerados como acionadores para o analisador heurístico.
9. Na seção **Detecção de login de rede**, indique o início e o fim do intervalo de tempo durante o qual o Kaspersky Embedded Systems Security 2.2 encara tentativas de login como atividades anormais.
10. Selecione a guia **Exclusões**.
11. Execute as seguintes ações para adicionar usuários confiáveis:
    a. Clique no botão **Procurar**.
    b. Selecione um usuário.
    c. Clique em **OK**.

    Um usuário selecionado é adicionado à lista de usuários confiáveis.
12. Execute as seguintes ações para adicionar endereços IP confiáveis:
    a. Insira o endereço IP.
    b. Clique no botão **Adicionar**.
13. Um endereço IP inserido é adicionado à lista de endereços IP confiáveis.
14. Na guia **Gerenciamento de tarefa** configure a programação de início da tarefa (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 122).
15. Clique em **OK**.

A configuração da tarefa de Inspeção do Log é salva.

Configuração de regras de Inspeção do Log

► *Execute as seguintes ações para adicionar e configurar uma nova regra personalizada de Inspeção do log:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configurando políticas" na página 90).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).

   > Se um dispositivo estiver sendo gerenciado por uma política do Kaspersky Security Center ativa e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

3. Na seção **Inspeção do sistema**, clique no botão **Configurações** no bloco **Inspeção do Log**.

   A janela **Inspeção do Log** é exibida.
4. Na guia **Regras de Inspeção do Log**, marque ou desmarque a caixa de seleção **Aplicar regras personalizadas para a Inspeção do Log**.

   Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security 2.2 aplicará regras personalizadas à Inspeção do Log segundo as configurações de cada regra. É possível adicionar, remover ou configurar regras de Inspeção do Log.

   Se a caixa de seleção for desmarcada, você não poderá adicionar ou modificar as regras personalizadas. O Kaspersky Embedded Systems Security 2.2 aplica as configurações de regras padrão.

   A caixa de seleção é selecionada por padrão. Apenas a regra de Detecção de pop-up do aplicativo está ativa.

   > É possível controlar se as regras predefinidas serão aplicadas à Inspeção do Log. Marque as caixas de seleção correspondentes às regras que deseja aplicar à Inspeção do Log.

5. Para adicionar uma nova regra personalizada, clique no botão **Adicionar**.

   A janela **Regras de inspeção do log** é exibida.
6. Na seção **Geral**, insira as seguintes informações sobre a nova regra:
   - **Nome**
   - **Origem**

Selecione um log de fonte para utilizar eventos registrados para a análise. Os seguintes tipos de log de eventos do Windows estão disponíveis:

- Aplicativo
- Segurança
- Sistema

Você pode adicionar um novo log personalizado inserindo o nome do log no campo **Origem**.

7. Na seção **ID de eventos acionados**, especifique os IDs do item que acionará a regra na detecção:

   a. Insira um valor numérico para os IDs.

   b. Clique no botão **Adicionar**.

   Um ID de regra selecionado é adicionado à lista. É possível adicionar um número ilimitado de identificadores para cada regra.

   c. Clique em **OK**.

   A regra de Inspeção do Log é adicionada à lista de regras.

Relatórios do Kaspersky Security Center

Os relatórios do Kaspersky Security Center contêm informações sobre o status de dispositivos gerenciados. Os relatórios são baseados em informações armazenadas no Servidor de Administração.

A partir do Kaspersky Security Center 11, os seguintes tipos de relatórios estão disponíveis para o Kaspersky Embedded Systems Security 2.2:

- Relatório do status dos componentes do aplicativo
- Relatório de aplicativos proibidos
- Relatório de aplicativos proibidos em modo de teste

Consulte a *Ajuda do Kaspersky Security Center* para obter informações detalhadas sobre todos os relatórios do Kaspersky Security Center e como configurá-los.

Relatório do status dos componentes do aplicativo

É possível monitorar o status de proteção de todos os dispositivos da rede e obter um resumo estruturado do conjunto de componentes em cada dispositivo.

O relatório exibe um dos seguintes estados de cada componente: *Executando, Pausado, Interrompido, Mau funcionamento, Não instalado, Iniciando*.

O status *Não instalado* refere-se ao componente, não ao próprio aplicativo. Se o aplicativo não estiver instalado, o Kaspersky Security Center atribui o status N/A (Não disponível).

É possível criar seleções de componentes e usar filtros para exibir dispositivos de rede com o conjunto de componentes definidos e o estado deles.

Consulte a *Ajuda do Kaspersky Security Center* para obter informações detalhadas sobre a criação e o uso das seleções.

► *Para revisar o status dos componentes nas configurações do aplicativo:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definindo tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 101).
3. Selecione a seção **Componentes**.
4. Revise a tabela de status.

► *Para revisar um relatório padrão do Kaspersky Security Center:*

1. Selecione o nó **Servidor de Administração <Nome de computador>** na árvore do Console de Administração.
2. Abra a guia **Relatórios**.
3. Clique duas vezes no item da lista **Relatório do status de componentes do aplicativo**.

   Um relatório é gerado.
4. Revise os seguintes detalhes do relatório:
   - Um diagrama gráfico.
   - Uma tabela de resumo de componentes e números agregados de dispositivos da rede em que cada componente está instalado, e grupos aos quais pertencem.
   - Uma tabela detalhada especificando o status, a versão, o dispositivo e o grupo do componente.

Relatórios de aplicativos bloqueados em modos ativo e de estatística

Baseado nos resultados da execução da tarefa de Controle de Inicialização de Aplicativos (consulte a seção "Gerenciando a inicialização de aplicativos do Kaspersky Security Center" na página 175), dois tipos de relatórios podem ser gerados: o relatório de aplicativos proibidos (se a tarefa for iniciada no modo **Ativa**) e o relatório de aplicativos proibidos no modo de teste (se a tarefa for iniciada no modo **Somente estatísticas**). Estes relatórios exibem informações sobre aplicativos bloqueados nos servidores protegidos da rede. Cada relatório é gerado para todos os grupos de administração e acumula dados de todos os aplicativos da Kaspersky Lab instalados nos dispositivos protegidos.

► *Para revisar um relatório de aplicativos proibidos no modo de teste:*

1. Inicie a tarefa de Controle de Aplicativos no modo Somente estatísticas (consulte a seção "Definição de configurações da tarefa de Controle de Inicialização de Aplicativos" na página 177).
2. Selecione o nó **Servidor de Administração <Nome de computador>** na árvore do Console de Administração.
3. Abra a guia **Relatórios**.
4. Clique duas vezes no item da lista **Relatório de aplicativos proibidos em modo de teste**.

   Um relatório é gerado.
5. Revise os seguintes detalhes do relatório:
   - Um diagrama gráfico exibe os dez principais aplicativos com o maior número de inicializações bloqueadas.
   - Uma tabela de resumo de bloqueios do aplicativo especificando o nome do arquivo executável, o motivo, o horário do bloqueio e o número de dispositivos em que o bloqueio ocorreu.
   - Uma tabela detalhada especificando dados do dispositivo, o caminho do arquivo e os critérios de bloqueio.

► *Para revisar um relatório de aplicativos proibidos no modo Ativo:*

1. Inicie a tarefa de Controle de Aplicativos no modo Ativa (consulte a seção "Definição de configurações da tarefa de Controle de Inicialização de Aplicativos" na página 177),
2. Selecione o nó **Servidor de Administração <Nome de computador>** na árvore do Console de Administração.
3. Abra a guia **Relatórios**
4. Clique duas vezes no item da lista **Relatório de aplicativos proibidos**.

   Um relatório é gerado.

Este relatório contém os mesmos blocos de dados que o relatório de aplicativos proibidos no modo de teste.

Trabalhando com o Kaspersky Embedded Systems Security 2.2 a partir da linha de comando

Esta seção descreve como trabalhar com o Kaspersky Embedded Systems Security 2.2 a partir da linha de comando.

Neste capítulo

Comandos da linha de comando

Você poderá executar comandos de gerenciamento básico do Kaspersky Embedded Systems Security 2.2 na linha de comando do computador protegido, se tiver incluído o componente Utilitário de linha de comando na lista de recursos instalados durante a instalação do Kaspersky Embedded Systems Security 2.2.

Usando os comandos da linha de comando, você pode gerenciar apenas funções às quais tem acesso, de acordo com as permissões atribuídas a você no Kaspersky Embedded Systems Security 2.2.

Certos comandos do Kaspersky Embedded Systems Security 2.2 são executados da seguinte maneira:

- Modo síncrono: o gerenciamento volta ao Console somente após a conclusão da execução do comando.
- Modo assíncrono: o gerenciamento volta ao Console imediatamente após a execução do comando.

► *Para interromper a execução de um comando no modo síncrono*

Pressione a combinação de teclas de atalho no teclado **Ctrl+C**.

Observe as seguintes regras ao inserir comandos do Kaspersky Embedded Systems Security 2.2:

- Introduza modificadores e comandos usando letras maiúsculas e minúsculas.
- Delimite modificadores com o caractere de espaço.
- Se o nome do arquivo/pasta cujo caminho você especificar como valor chave incluir um espaço, especifique o caminho do arquivo/pasta entre aspas, por exemplo: `"C:\TEST\test cpp.exe"`
- Se necessário, use os marcadores de posição no nome do arquivo ou máscaras de caminho, por exemplo: “`C:\Temp\Temp*\`”, “`C:\Temp\Temp???.doc`”, “`C:\Temp\Temp*.doc`”

Você pode usar a linha de comandos para todo o conjunto de operações requeridas para gerenciamento e administração do Kaspersky Embedded Systems Security 2.2 (consulte a tabela abaixo).

Tabela 38. Comandos do Kaspersky Embedded Systems Security 2.2

Comando	Descrição
KAVSHELL APPCONTROL (consulte a seção "Preenchendo a lista de regras de Controle de inicialização de aplicativos KAVSHELL APPCONTROL" na página 238)	Renova a lista de regras especificadas de acordo com o princípio de adição selecionado.
KAVSHELL APPCONTROL/CONFIG (consulte a seção "Gerenciamento da tarefa de Controle de Inicialização de Aplicativos KAVSHELL APPCONTROL /CONFIG" na página 236)	Controla o modo operacional da tarefa de Controle de Inicialização de Aplicativos
KAVSHELL APPCONTROL /GENERATE (consulte a seção "Gerador de Regras de Controle de Inicialização de Aplicativos KAVSHELL APPCONTROL /GENERATE" na página 236)	Inicia a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos.
KAVSHELL VACUUM (consulte a seção "Desfragmentação de arquivos de log do Kaspersky Embedded Systems Security 2.2. KAVSHELL VACUUM" na página 247)	Desfragmenta arquivos de log do Kaspersky Embedded Systems Security 2.2.
KAVSHELL PASSWORD	Gerencia as configurações de proteção de senha.
KAVSHELL HELP (consulte a seção "Exibindo a ajuda de comando do Kaspersky Embedded Systems Security 2.2. KAVSHELL HELP" na página 228)	Exibe a ajuda do comando para o Kaspersky Embedded Systems Security 2.2.
KAVSHELL START (consulte a seção "Iniciando e interrompendo o Kaspersky Security Service KAVSHELL START, KAVSHELL STOP" na página 229)	Inicia o serviço Kaspersky Embedded Systems Security 2.2.
KAVSHELL STOP (consulte a seção "Iniciando e interrompendo o Kaspersky Security Service KAVSHELL START, KAVSHELL STOP" na página 229)	Interrompe o serviço do Kaspersky Embedded Systems Security 2.2.
KAVSHELL SCAN (consulte a seção "Verificação da área selecionada. KAVSHELL SCAN" na página 229)	Cria e inicia uma tarefa de Verificação por Demanda temporária com o escopo da verificação e as configurações de segurança especificadas pelos modificadores do comando.
KAVSHELL SCANCRITICAL (consulte a seção "Iniciando a tarefa de Verificação de áreas críticas. KAVSHELL SCANCRITICAL" na página 233)	Inicia a tarefa do sistema de Verificação de áreas críticas.
KAVSHELL TASK (consulte a seção "Gerenciando a tarefa especificada de maneira assíncrona. KAVSHELL TASK" na página 234)	Inicia/pausa/reinicia/interrompe a tarefa selecionada de forma assíncrona/retorna o status/estatísticas da tarefa atual.
KAVSHELL RTP (consulte a seção "Inicialização e interrupção de tarefas de Proteção em tempo real. KAVSHELL RTP" na página 235)	Executa ou interrompe todas as tarefas de Proteção em tempo real.
KAVSHELL UPDATE (consulte a seção "Iniciando a tarefa de Atualização do Banco de Dados do Kaspersky Embedded Systems Security 2.2. KAVSHELL UPDATE" na página 240)	Inicia a tarefa de atualização de bancos de dados do Kaspersky Embedded Systems Security 2.2 com as configurações especificadas usando modificadores de comando.

Comando	Descrição
KAVSHELL REVERTEM (consulte a seção "Revertendo atualizações do banco de dados do Kaspersky Embedded Systems 2.2. KAVSHELL ROLLBACK" na página 244)	Reverte os bancos para a versão anterior.
KAVSHELL LICENSE (consulte a seção "Ativando o aplicativo KAVSHELL LICENSE" na página 244)	Gerencia chaves.
KAVSHELL TRACE (consulte a seção "Ativando, configurando e desativando o log de rastreamento. KAVSHELL TRACE" na página 246)	Ativa ou desativa o log de rastreamento, gerencia as configurações do log de rastreamento.
KAVSHELL DUMP (consulte a seção "Ativando e desativando a criação do arquivo de despejo. KAVSHELL DUMP" na página 248)	Ativa ou desativa os arquivos de despejo da memória de processo do Kaspersky Embedded Systems Security 2.2 no caso de encerramento anormal de processos.
KAVSHELL IMPORT (consulte a seção "Importando configurações. KAVSHELL IMPORT" na página 249)	Importa configurações, funções e tarefas gerais do Kaspersky Embedded Systems Security 2.2 de um arquivo de configuração criado anteriormente.
KAVSHELL EXPORT (consulte a seção "Exportando configurações. KAVSHELL EXPORT" na página 250)	Exporta todas as configurações e tarefas existentes do Kaspersky Embedded Systems Security 2.2 para um arquivo de configuração.
KAVSHELL DEVCONTROL (consulte a seção "Preenchimento da lista de regras de Controle de Dispositivos. KAVSHELL DEVCONTROL" na página 239)	Adiciona à lista de regras de controle de dispositivos gerada de acordo com o método selecionado.

Exibindo a ajuda de comando do Kaspersky Embedded Systems Security. 2.2 KAVSHELL HELP

Para obter a lista de todos os comandos do Kaspersky Embedded Systems Security 2.2, execute um dos comandos a seguir:

```
KAVSHELL
KAVSHELL HELP
KAVSHELL /?
```

Para obter uma descrição de um comando e sua sintaxe, execute um dos comandos a seguir:

```
KAVSHELL HELP <comando>
KAVSHELL <comando> /?
```

Exemplos de comando KAVSHELL HELP

Para exibir informações detalhadas sobre o comando KAVSHELL SCAN, execute o seguinte comando:

```
KAVSHELL HELP SCAN
```

Iniciando e interrompendo o Kaspersky Security Service KAVSHELL START, KAVSHELL STOP

Para executar o Kaspersky Security Service, execute o comando

```
KAVSHELL START
```

Por padrão, quando o Kaspersky Security Service é iniciado, as tarefas de Proteção de Arquivos em Tempo Real e Verificação na inicialização do sistema, bem como outras tarefas programadas para iniciar **Ao iniciar o aplicativo** serão iniciadas.

Para interromper o Kaspersky Security Service, execute o comando

```
KAVSHELL STOP
```

A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Verifica a área selecionada. KAVSHELL SCAN

Para iniciar uma tarefa para verificar áreas específicas do computador protegido use o comando `KAVSHELL SCAN`. Os modificadores de comando especificam o escopo da verificação e as configurações de segurança do nó selecionado.

A tarefa de Verificação por Demanda iniciada usando o comando `KAVSHELL SCAN` é uma tarefa temporária. Ela é exibida no Console do Aplicativo apenas enquanto é executada (não é possível visualizar as configurações da tarefa no Console do Aplicativo). O log de desempenho da tarefa é gerado simultaneamente. Ele é exibido em **Logs de tarefas** no Console do Aplicativo.

Ao especificar caminhos em tarefas de verificação para áreas específicas, você pode usar variáveis de ambiente. Se você usar a variável de ambiente especificada para o usuário, execute o comando `KAVSHELL SCAN` com as permissões para esse usuário.

O comando `KAVSHELL SCAN` é executado no modo síncrono.

Para iniciar uma tarefa de Verificação por Demanda existente a partir da linha de comando, use o comando KAVSHELL TASK (consulte a seção "Gerenciando a tarefa especificada de maneira assíncrona.Comando KAVSHELL TASK" na página 234).

Sintaxe do comando KAVSHELL SCAN

```
KAVSHELL SCAN <escopo da verificação> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|
/FIXDRIVES|/MYCOMP] [/L:< caminho do arquivo com a lista de escopos
da verificação >] [/F<A|C|E>] [/NEWONLY] [/AI:<DISINFECT|DISINFDEL|DELETE|
REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE]
[/E:<ABMSPO>] [/EM:<"máscaras">] [/ES:<tamanho>] [/ET:<número de segundos>]
[/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<dias>] [NORECALL]>] [/NOICHECKER]
[/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<caminho para o arquivo de log
```

```
de tarefas>] [/ANSI] [/ALIAS:<alias da tarefa>]
```

O comando KAVSHELL SCAN tem chaves obrigatórias e opcionais (veja a tabela abaixo).

Exemplos do comando KAVSHELL SCAN

```
KAVSHELL SCAN Pasta56 D:\Pasta1\Pasta2\Pasta3\ C:\Pasta1\ C:\Pasta2\3.exe
“\\outro servidor\Shared\” F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
/E:ABM /EM:”*.xtx;*.fff;*.ggg;*.bbb;*.info” /NOICHECKER /ANALYZERLEVEL:1
/NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Tabela 39. Modificadores do comando KAVSHELL SCAN

Chave	Descrição
Escopo da verificação. Modificador obrigatório.	
<arquivos> <pastas> <caminho de rede>	Especifica o escopo da verificação - lista de arquivos, pastas, caminhos de rede e áreas predefinidas. Especifique os caminhos de rede no formato UNC (Universal Naming Convention). No exemplo seguinte, a pasta Pasta4 é especificada sem um caminho - ela está localizada na pasta a partir da qual você inicia o comando KAVSHELL: KAVSHELL SCAN Pasta4 Se o nome do objeto a ser verificado contiver espaços, ele deverá ser colocado entre aspas. Quando uma pasta for selecionada, o Kaspersky Embedded Systems Security 2.2 também verificará todas as subpastas dessa pasta. Os símbolos * ou ? podem ser usados para verificar um grupo de arquivos.
/MEMORY	Verifica objetos da RAM
/SHARED	Verifica pastas compartilhadas do computador
/STARTUP	Verifica objetos de inicialização
/REMDRIVES	Verifica unidades removíveis
/FIXDRIVES	Verifica discos rígidos
/MYCOMP	Verifica todas as áreas do computador protegido
/L:<caminho do arquivo com a lista de escopos da verificação>	Nome do arquivo com a lista de escopos da verificação, incluindo o caminho completo do arquivo. Delimita os escopos da verificação nos arquivos usando quebras de linha. Você pode especificar áreas de verificação predefinidas tal como é exibido no seguinte exemplo de um arquivo com uma lista do escopo da verificação: C:\ D:\Docs*.doc E:\Meus Documentos /STARTUP /SHARED
Objetos verificados (Tipos de arquivos). Se você não especificar valores para esse modificador, o Kaspersky Embedded Systems Security 2.2 verificará objetos pelo seu formato.	

Chave	Descrição
/FA	Verifica todos os objetos
/FC	Verifica objetos por formato (por padrão). O Kaspersky Embedded Systems Security 2.2 verifica somente o formato dos objetos incluídos na lista de formatos de objetos infectáveis.
/FE	Verifica objetos por extensão. O Kaspersky Embedded Systems Security 2.2 verifica somente objetos com extensões incluídas na lista de extensões de objetos infectáveis.
/NEWONLY	Verifica apenas arquivos novos e modificados. Se você não fornecer esse modificador, o Kaspersky Embedded Systems Security 2.2 verificará todos os objetos.
Ação a ser executada em objetos infectados e em outros objetos. Se você não especificar valores para esse modificador, o Kaspersky Embedded Systems Security 2.2 executará a ação **Ignorar**.	
DISINFECT	Desinfectar; ignorar se a desinfecção não for possível
DISINFDEL	Desinfectar; excluir se a desinfecção não for possível
DELETE	Excluir As configurações DISINFECT e DELETE são salvas na versão atual do Kaspersky Embedded Systems Security 2.2 para garantir a compatibilidade com versões anteriores. Essas configurações podem ser utilizadas em vez dos comandos da chave /AI: e /AS: Neste caso, o Kaspersky Embedded Systems Security 2.2 não processará os objetos possivelmente infectados.
REPORT	Enviar relatório (por padrão)
AUTO	Executar ação recomendada
/AS: **Ação a ser executada em objetos possivelmente infectados**/ Se você não especificar valores para esse modificador, o Kaspersky Embedded Systems Security 2.2 executará a ação **Ignorar**.	
QUARANTINE	Quarentena
DELETE	Excluir
REPORT	Enviar relatório (por padrão)
AUTO	Executar ação recomendada
Exclusões	
/E:ABMSPO	Exclui objetos compostos dos seguintes tipos: A – arquivos compactados (verifica apenas arquivos compactados SFX) B – bancos de dados de e-mail M – e-mail sem formatação S – arquivos compactados e arquivos compactados SFX P – objetos compactados O – objetos OLE incorporados
/EM:<”máscaras”>	Excluir arquivos por máscara É possível especificar várias máscaras, por exemplo: EM:”*.txt;*.png; C\Videos*.avi”.

Chave	Descrição
/ET:<número de segundos>	Interrompe o processamento do objeto se ele continuar para além do número de segundos especificado pelo valor <número de segundos>. Por padrão, não há uma restrição de tempo.
/ES:<tamanho>	Não verificar objetos compostos maiores do que o tamanho (em MB) especificado pelo valor <tamanho>. Por padrão, o Kaspersky Embedded Systems Security 2.2 verifica objetos de todos os tamanhos.
/TZOFF	Desativa exclusões da Zona Confiável
Configurações avançadas (Opções)	
/NOICHECKER	Desativa o uso da tecnologia iChecker (ativado por padrão)
/NOISWIFT	Desativa o uso da tecnologia iSwift (ativado por padrão)
/ANALYZERLEVEL:<intensidade da análise>	Ativa o Analisador Heurístico, configura o nível de análise. Estão disponíveis os seguintes níveis de análise heurística: 1 – superficial 2 – médio 3 – profundo Se você omitir o modificador, o Kaspersky Embedded Systems Security 2.2 não usará o analisador heurístico.
/ALIAS:<alias da tarefa>	Permite atribuir a uma tarefa de Verificação por Demanda um nome temporário através do qual a tarefa pode ser acessada durante sua execução, por exemplo para visualizar as estatísticas usando o comando TASK. O alias da tarefa deve ser exclusivo entre os aliases de tarefas de todos os componentes funcionais do Kaspersky Embedded Systems Security 2.2. Se esse modificador não for especificado, é usado o nome temporário scan_<kavshell_pid>, por exemplo, scan_1234. No Console do Aplicativo, a tarefa recebe o nome Scan objects (<data e hora>), por exemplo, Scan objects 16/08/2007 17h13m14.
Configurações dos logs de tarefas (Configurações de relatórios)	

Chave	Descrição
/W:<caminho do arquivo de log de tarefas>	Se esta chave for especificada, o Kaspersky Embedded Systems Security 2.2 salvará o arquivo de log de tarefas com o nome definido pelo valor da chave. O arquivo de log contém estatísticas de execução da tarefa, a hora em que ela foi iniciada e concluída (interrompida), além de informações sobre os eventos da tarefa. O log é usado para registrar eventos definidos pelas configurações de log de tarefas e pelo log de eventos do Kaspersky Embedded Systems Security 2.2 no "Visualizador de Eventos". É possível especificar o caminho absoluto ou relativo do arquivo de log. Se você especificar somente o nome de um arquivo sem especificar o caminho respetivo, o arquivo de log será criado na pasta atual. Ao reiniciar o comando com as mesmas configurações de log, o arquivo de log existente será substituído. O arquivo de log pode ser exibido enquanto uma tarefa está em execução. O log é exibido no nó Logs de tarefa do Console do Aplicativo. Se o Kaspersky Embedded Systems Security 2.2 não conseguir criar o arquivo de log, ele não irá interromper a execução do comando, mas exibirá uma mensagem de erro.
/ANSI	A opção permite registrar os eventos no log de tarefas com a codificação ANSI. A opção ANSI não será aplicada se a opção W não for definida. Se a opção ANSI não for especificada, o log de tarefas é gerado usando a codificação UNICODE.

Iniciando a tarefa de Verificação de áreas críticas. KAVSHELL SCANCRITICAL

Use o comando `KAVSHELL SCANCRITICAL` para iniciar a tarefa do sistema Verificação por Demanda do sistema e Verificação de áreas críticas com as configurações definidas no Console do Aplicativo.

Sintaxe do comando KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<caminho para o arquivo de log de tarefas>]
```

Exemplos do comando KAVSHELL SCANCRITICAL

Para executar a tarefa de Verificação por Demanda e de Verificação de Áreas Críticas e salvar o log de tarefas scancritical.log na pasta atual, execute o seguinte comando:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Dependendo da sintaxe do modificador /W, você pode configurar a localização do log de tarefas (consulte a tabela abaixo).

Tabela 40. Sintaxe do modificador /W para o comando KAVSHELL SCANCRITICAL

Chave	Descrição
/W:<caminho do arquivo de log de tarefas>	Se esta chave for especificada, o Kaspersky Embedded Systems Security 2.2 salvará o arquivo de log de tarefas com o nome definido pelo valor da chave. O arquivo de log contém estatísticas de execução da tarefa, a hora em que ela foi iniciada e concluída (interrompida), além de informações sobre os eventos da tarefa. O log é usado para registrar eventos definidos pelas configurações de logs de tarefas e pelo log de eventos do aplicativo no Visualizador de Eventos. É possível especificar o caminho absoluto ou relativo do arquivo de log. Se você especificar somente o nome de um arquivo sem especificar o caminho respetivo, o arquivo de log será criado na pasta atual. Ao reiniciar o comando com as mesmas configurações de log, o arquivo de log existente será substituído. O arquivo de log pode ser exibido enquanto uma tarefa está em execução. O log é exibido no nó **Logs de tarefa** do Console do Aplicativo. Se o Kaspersky Embedded Systems Security 2.2 não conseguir criar o arquivo de log, ele não irá interromper a execução do comando, mas exibirá uma mensagem de erro.

Gerenciando a tarefa especificada de maneira assíncrona. KAVSHELL TASK

Usando o comando `KAVSHELL TASK` você pode gerenciar a tarefa especificada: executar, pausar, continuar e interromper a tarefa especificada e visualizar o status e as estatísticas da tarefa atual. Este comando é executado no modo assíncrono.

> A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL TASK

```
KAVSHELL TASK [<alias do nome da tarefa> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Exemplos do comando KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE
```

O comando `KAVSHELL TASK` pode ser executado sem modificadores ou com um ou vários modificadores (consulte a tabela abaixo).

Tabela 41. Modificadores do comando KAVSHELL TASK

Chave	Descrição
Sem chaves	Retorna a lista de todas as tarefas existentes do Kaspersky Embedded Systems Security 2.2. A lista contém os campos: nome alternativo da tarefa, categoria da tarefa (sistema ou personalizada) e status atual da tarefa.
<alias da tarefa>	Em vez do nome da tarefa, no comando SCAN TASK, use o alias da tarefa, um nome abreviado adicional atribuído pelo Kaspersky Embedded Systems Security 2.2 às tarefas. Para visualizar os aliases de tarefa do Kaspersky Embedded Systems Security 2.2 insira o comando KAVSHELL TASK sem modificadores
/START	Inicia a tarefa especificada no modo assíncrono.
/STOP	Interrompe a tarefa especificada.
/PAUSE	Pausa a tarefa especificada.
/RESUME	Reinicia a tarefa especificada no modo assíncrono.
/STATE	Retorna o status da tarefa atual (por exemplo, **Executando**, **Concluída**, **Pausada**, **Interrompida**, **Falhou**, **Iniciando**, **Recuperando**).
/STATISTICS	Obtém as estatísticas da tarefa - informações sobre o número de objetos processados a partir da hora de início da tarefa até agora.

Os códigos de retorno do comando KAVSHELL TASK (consulte a seção "Códigos de retorno do comando KAVSHELL TASK" na página 253).

Inicialização e interrupção de tarefas de Proteção em Tempo Real. KAVSHELL RTP

Usando o comando `KAVSHELL RTP` você pode iniciar ou parar todas as tarefas de proteção em tempo real.

> A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Exemplos do comando KAVSHELL RTP

Para executar tarefas de proteção em tempo real, execute o seguinte comando:

```
KAVSHELL RTP /START
```

O comando `KAVSHELL RTP` pode incluir qualquer dos dois modificadores obrigatórios (consulte a tabela abaixo).

Tabela 42. Modificadores do comando KAVSHELL RTP

Chave	Descrição
/START	Inicia todas as tarefas de Proteção em Tempo Real: Proteção de Arquivos em Tempo Real e Uso da KSN.
/STOP	Interrompe todas as tarefas de proteção em tempo real.

Gerenciamento da tarefa de Controle de Inicialização de Aplicativos KAVSHELL APPCONTROL /CONFIG

É possível usar o comando `KAVSHELL APPCONTROL /CONFIG` para configurar o modo em que a tarefa de Controle de Inicialização de Aplicativos executa e monitora o carregamento de módulos DLL.

Sintaxe do comando KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
/savetofile:<caminho completo para o arquivo XML>
```

Exemplos do comando KAVSHELL APPCONTROL /CONFIG

► *Para executar a tarefa de Controle de Inicialização de Aplicativos no modo **Ativa** sem carregar uma DLL e salvar as configurações da tarefa após a conclusão, execute o comando a seguir:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Você pode definir as configurações da tarefa de Controle de Inicialização de Aplicativos usando os parâmetros de linha de comando (consulte a tabela abaixo).

Tabela 43. Chaves de comando `KAVSHELL APPCONTROL /GENERATE`

Chave	Descrição
`/mode:<applyrules|statistics>`	Modo operacional da tarefa de Controle de Inicialização de Aplicativos. Você pode selecionar um dos seguintes modos: • ativa - aplicar regras de Controle de Inicialização de Aplicativos; • estatísticas - Somente estatísticas.
`/dll:<no|yes>`	Ativa ou desativa o monitoramento do carregamento de DLL.
`/savetofile: <caminho para arquivo XML>`	Exporta as regras especificadas no arquivo indicado no formato XML.
`/savetofile: <nome completo do arquivo xml>`	Salva a lista de regras no arquivo.
`/savetofile: <nome completo do arquivo xml> /sdc`	Salva a lista de regras do Controle de Distribuição de Software no arquivo.
`/clearsdc`	Exclui todas as regras de Controle de Distribuição de Software da lista.

Gerador de Regras de Controle de Inicialização de Aplicativos KAVSHELL APPCONTROL /GENERATE

Usando o comando `KAVSHELL APPCONTROL /GENERATE`, você pode gerar as listas de regras de Controle de inicialização de aplicativos.

> A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <caminho para a pasta> | /source:<caminho para o arquivo com lista de pastas> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<usuário ou grupo de usuários>] [/export:<caminho para arquivo XML>] [/import:<a|r|m>] [/prefix:<prefixo para nomes de regras>] [/unique]
```

Exemplos do comando KAVSHELL APPCONTROL /GENERATE

► *Para gerar regras para arquivos a partir de pastas especificadas, execute o comando a seguir:*

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

► *Para gerar regras para arquivos executáveis de todas as extensões disponíveis na pasta especificada e, após a conclusão de tarefa, salvar as regras geradas no arquivo XML do arquivo especificado, execute o seguinte comando:*

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
/export:c\rules\appctrlrules.xml
```

Dependendo da sintaxe das chaves você pode definir as configurações de geração de regras automáticas da tarefa de Controle de Inicialização de Aplicativos (consulte a tabela abaixo).

Tabela 44. Chaves do comando KAVSHELL APPCONTROL /GENERATE

Chave	Descrição
Escopo de uso das regras de permissão	
<caminho da pasta>	Especifica o caminho da pasta com arquivos executáveis que necessitam de regras de permissão geradas automaticamente.
/source: <caminho para o arquivo com lista de pastas>	Especifica o caminho do arquivo TXT com a lista de pastas contendo arquivos executáveis que necessitam de regras de permissão geradas automaticamente.
/masks: <edms>	Especifica extensões de arquivos executáveis que necessitam de regras de permissão geradas automaticamente. Você pode incluir em arquivos de escopo de uso das regras as seguintes extensões: • e - Arquivos EXE • d - Arquivos DLL • m - Arquivos MSI • s - scripts

<table>
<tr><th>Chave</th><th>Descrição</th></tr>
<tr><td>/runapp</td><td>Ao gerar regras de permissão, leva em consideração aplicativos em execução em um computador protegido no momento da execução da tarefa.</td></tr>
<tr><td colspan="2">Ações ao gerar regras de permissão automaticamente</td></tr>
<tr><td>/rules: <ch|cp|h></td><td>Especifica ações a serem executadas durante a geração de regras de permissão de Controle de inicialização de aplicativos: ch - usar certificado digital. Se o certificado estiver em falta, utilize o hash SHA256. cp - usar o certificado digital. Se o certificado estiver em falta, use o caminho ao arquivo executável. h - usar hash SHA256.</td></tr>
<tr><td>/strong</td><td>Usa o assunto e a miniatura do certificado digital ao gerar automaticamente as regras de permissão de Controle de inicialização de aplicativos.
O comando é executado se a chave /rules: <ch|cp> for especificada.</td></tr>
<tr><td>/user: <usuário ou grupo de usuários></td><td>Especifica o nome de usuário ou de um grupo de usuários para os quais as regras serão aplicadas. O aplicativo controlará qualquer aplicativo executado pelo usuário e/ou grupo de usuários especificado.</td></tr>
<tr><td colspan="2">Ações na conclusão do Gerador de Regras de Controle de Inicialização de Aplicativos</td></tr>
<tr><td>/export: <path to XML file></td><td>Salva as regras geradas no arquivo XML.</td></tr>
<tr><td>/unique</td><td>Adiciona informações sobre o computador com aplicativos instalados que são a base para a geração de regras de permissão de Controle de inicialização de aplicativos.</td></tr>
<tr><td>/prefix: <prefixo para nomes de regras></td><td>Especifica o prefixo de nome para a geração de regras de permissão de controle de inicialização de aplicativos.</td></tr>
<tr><td>/import: <a|r|m></td><td>Importa regras geradas à lista de regras de controle de inicialização de aplicativos especificadas de acordo com o princípio de adição selecionado. : a - Adicionar às regras existentes (regras com configurações idênticas são duplicadas) r - Substituir as regras existentes (regras com parâmetros idênticos não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único) m - Mesclar com as regras existentes (regras com parâmetros idênticos não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único)</td></tr>
</table>

Preenchendo a lista de regras de Controle de inicialização de aplicativos KAVSHELL APPCONTROL

Utilizando `KAVSHELL APPCONTROL`, é possível adicionar regras do arquivo XML na lista de regras da tarefa de Controle de Inicialização de Aplicativos de acordo com o princípio selecionado e também excluir todas as regras definidas da lista.

A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <caminho para arquivo XML> | /replace <caminho
para arquivo XML> | /merge <caminho para arquivo XML> | /clear
```

Exemplos do comando KAVSHELL APPCONTROL

► *Para adicionar regras de um arquivo XML às regras já especificadas para a tarefa de Controle de Inicialização de Aplicativos de acordo com o princípio Adicionar às regras existentes, execute o seguinte comando:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

Dependendo da sintaxe das chaves, você pode selecionar o princípio para adicionar novas regras um arquivo XML especificado a uma lista de regras definidas do Controle de inicialização de aplicativos (consulte a tabela abaixo).

Tabela 45. Chaves do comando `KAVSHELL SCAN`

Chave	Descrição
/append <caminho para arquivo XML>	Renova a lista de regras de controle de inicialização de aplicativos com base em um arquivo XML especificado. Princípio de adição - **Adicionar às regras existentes** (regras com configurações idênticas são duplicadas).
/replace <caminho para arquivo XML>	Renova a lista de regras de controle de inicialização de aplicativos com base em um arquivo XML especificado. Princípio de adição - **Substituir as regras existentes** (regras com parâmetros idênticos não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único).
/merge <caminho para arquivo XML>	Renova a lista de regras de controle de inicialização de aplicativos com base em um arquivo XML especificado. Princípio de adição - **Mesclar com as regras existentes** (as novas regras não duplicam as regras já existentes).
/clear	Apaga a lista de regras de Controle de inicialização de aplicativos.

Preenchimento da lista de regras de Controle de Dispositivos. KAVSHELL DEVCONTROL

Utilizando `KAVSHELL DEVCONTROL` , é possível adicionar regras do arquivo XML à lista de regras da tarefa de Controle de Dispositivos de acordo com o princípio selecionado e também excluir todas as regras definidas da lista.

A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <caminho para arquivo XML> | /replace <caminho
para arquivo XML> | /merge <caminho para arquivo XML> | /clear
```

Exemplos do comando KAVSHELL DEVCONTROL

► *Para adicionar regras de um arquivo XML às regras já especificadas para a tarefa de Controle de Dispositivos de acordo com o princípio **Adicionar às regras existentes**, execute o seguinte comando:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

Dependendo da sintaxe das chaves, você pode selecionar o princípio para adicionar novas regras e um arquivo XML especificado a uma lista de regras definidas do Controle de dispositivos (consulte a tabela abaixo).

Tabela 46. Chaves do comando KAVSHELL DEVCONTROL

Chave	Descrição
/append <caminho para arquivo XML>	Renova a lista de regras de controle de dispositivos com base em um arquivo XML especificado. Princípio de adição - **Adicionar às regras existentes** (regras com configurações idênticas são duplicadas).
/replace <caminho para arquivo XML>	Renova a lista de regras de controle de dispositivos com base em um arquivo XML especificado. Princípio de adição - **Substituir as regras existentes** (regras com parâmetros idênticos não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único).
/merge <caminho para arquivo XML>	Renova a lista de regras de controle de dispositivos com base em um arquivo XML especificado. Princípio de adição - **Mesclar com as regras existentes** (as novas regras não duplicam as regras já existentes).
/clear	Apaga a lista de regras de Controle de Dispositivos.

Iniciando a tarefa de atualização dos bancos de dados do Kaspersky Embedded Systems Security 2.2. KAVSHELL UPDATE

O comando `KAVSHELL UPDATE` pode ser usado para executar a atualização dos bancos de dados do Kaspersky Embedded Systems Security 2.2 no modo assíncrono.

A tarefa de atualização dos bancos de dados do Kaspersky Embedded Systems Security 2.2 executada usando o comando `KAVSHELL UPDATE` é uma tarefa temporária. Ela é exibida apenas no Console do Aplicativo ao ser executada. O log de tarefas é gerado simultaneamente. Ele é exibido em **Logs de tarefas** no Console do Aplicativo. As políticas do Kaspersky Security Center podem ser aplicadas às tarefas de atualização criadas e iniciadas usando o comando `KAVSHELL UPDATE` e as tarefas de atualização criadas no Console do Aplicativo. Para obter informações sobre o gerenciamento do Kaspersky Embedded Systems Security 2.2 em computadores usando o Kaspersky Security Center, consulte a seção "Gerenciando o Kaspersky Embedded Systems Security 2.2 usando o Kaspersky Security Center".

É possível usar variáveis de ambiente ao especificar o caminho da fonte de atualizações nesta tarefa. Se forem usadas variáveis de ambiente do usuário, execute o comando `KAVSHELL UPDATE` com as permissões para esse usuário.

Sintaxe de comando de KAVSHELL UPDATE

```
KAVSHELL UPDATE < Caminho da fonte das atualizações | /AK | /KL> [/NOUSEKL]
[/PROXY:<address>:<porta>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nome de usuário>]
[/PROXYPWD:<senha>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE]
[/TIMEOUT:<segundos>] [/REG:<código iso3166>] [/W:<caminho para arquivo de log
```

```
de tarefas>] [/ALIAS:<alias da tarefa>]
```

O comando KAVSHELL UPDATE tem chaves obrigatórias e opcionais (veja a tabela abaixo).

Exemplos do comando KAVSHELL UPDATE

► *Para iniciar uma tarefa de atualização personalizada do banco de dados, execute o seguinte comando:*

```
KAVSHELL UPDATE
```

► *Para executar a tarefa de atualização do banco de dados usando os arquivos de atualização na pasta de rede \\server\databases, execute o seguinte comando:*

```
KAVSHELL UPDATE \\server\databases
```

► *Para iniciar uma tarefa de atualização do servidor FTP ftp://dnl-ru1.kaspersky-labs.com/ e registrar todos os eventos da tarefa no arquivo c:\update_report.log, execute o comando:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

► *Para baixar as atualizações do banco de dados do Kaspersky Embedded Systems Security 2.2 do servidor de atualização da Kaspersky Lab, conecte-se à fonte das atualizações por meio de um servidor proxy (endereço do servidor proxy: proxy.company.com, porta: 8080), para acessar o computador usando a autenticação NTLM integrada do Microsoft Windows com o nome de usuário: inetuser, senha: 123456, execute o seguinte comando:*

```
KAVSHELL UPDATE /KL /PROXY:proxy.empresa.com:8080 /AUTHTYPE:1
/PROXYUSER:inetuser /PROXYPWD:123456
```

Tabela 47. Chaves do comando KAVSHELL UPDATE

Chave	Descrição
Fonte das atualizações (chave obrigatória). Especifique uma ou várias fontes. O Kaspersky Embedded Systems Security 2.2 acessará as origens na ordem em que forem listadas. Delimite as origens com um espaço.	
<caminho em formato UNC>	Fonte de atualização definida pelo usuário. Caminho da pasta de atualização de rede no formato UNC.
<URL>	Fonte de atualizações definida pelo usuário. Endereço do servidor HTTP ou FTP no qual a pasta de atualização está localizada.
<Pasta local>	Fonte de atualizações definida pelo usuário. Pasta no computador protegido.
/AK	Servidor de administração do Kaspersky Security Center como a fonte da atualização.
/KL	Servidores de atualização da Kaspersky Lab como fonte das atualizações.
/NOUSEKL	Não use os servidores de atualização da Kaspersky Lab se não houver outras fontes de atualização disponíveis (usadas por padrão).
Configurações do servidor proxy	

Chave	Descrição
/PROXY:<endereço>:<porta>	Nome de rede ou endereço IP do servidor proxy e sua porta. Se esta chave não for especificada, o Kaspersky Embedded Systems Security 2.2 detectará automaticamente as configurações do computador proxy usado na rede local.
/AUTHTYPE:<0-2>	Esta chave especifica o método de autenticação para acessar o servidor proxy. Ele pode ter os seguintes valores: **0** – autenticação NTLM integrada do Microsoft Windows; o Kaspersky Embedded Systems Security 2.2 fará contato com o servidor proxy sob a conta **Sistema local** (**SYSTEM**) **1** – autenticação NTLM integrada do Microsoft Windows; o Kaspersky Embedded Systems Security 2.2 fará contato com o servidor proxy sob a conta com o nome de login e a senha especificados pelas chaves /PROXYUSER e /PROXYPWD **2** – autenticação com o nome de login e a senha especificados pelas chaves /PROXYUSER e /PROXYPWD (autenticação básica) Se não for exigida a autenticação para acessar o servidor proxy, não será necessário especificar uma chave.
/PROXYUSER:<nome de usuário>	O nome de usuário que será usado para acessar o servidor proxy. Se o valor da chave /AUTHTYPE:0 for especificado, as chaves /PROXYUSER:<nome de usuário> e /PROXYPWD:<senha> serão ignoradas.
/PROXYPWD:<senha>	A senha de usuário que será usada para acessar o servidor proxy. Se o valor da chave /AUTHTYPE:0 for especificado, as chaves /PROXYUSER:<nome de usuário> e /PROXYPWD:<senha> serão ignoradas. Se a chave /PROXYUSER for especificada e /PROXYPWD omitida, a senha será considerada como em branco.
/NOPROXYFORKL	Não usar as configurações do servidor proxy para se conectar aos servidores de atualização da Kaspersky Lab (usadas por padrão).
/USEPROXYFORCUSTOM	Usar as configurações do servidor proxy para se conectar às fontes de atualizações definidas pelo usuário (não usadas por padrão).
/USEPROXYFORLOCAL	Usar as configurações do servidor proxy para se conectar a fontes de atualização locais. Se não especificado, o valor **Ignorar o servidor proxy para endereços locais** será aplicado.
Configurações gerais do servidor FTP e HTTP	
/NOFTPPASSIVE	Se esta chave for especificada, o Kaspersky Embedded Systems Security 2.2 usará o modo de servidor FTP ativo para se conectar ao computador protegido. Se esta chave não for especificada, o Kaspersky Embedded Systems Security 2.2 usará o modo de servidor FTP passivo, se possível.
/TIMEOUT:<número de segundos>	Tempo limite de conexão com o servidor FTP ou HTTP. Se você não especificar esta chave, o Kaspersky Embedded Systems Security 2.2 usará o valor padrão: 10 segundos. O valor da chave deve ser um número inteiro.

Chave	Descrição
/REG:<código iso3166>	Configurações regionais. Esta chave é usada ao receber atualizações dos servidores de atualização da Kaspersky Lab. O Kaspersky Embedded Systems Security 2.2 otimiza a carga da atualização no computador protegido por meio da seleção do servidor de atualização mais próximo. Como valor desta chave, especifique o código da letra do país onde está localizado o computador protegido, de acordo com a ISO 3166-1, por exemplo, /REG: gr ou /REG:RU. Se esta chave for omitida ou um código de país não existente for especificado, o Kaspersky Embedded Systems Security 2.2 detectará a posição do computador protegido com base nas configurações regionais no computador onde o Console do Aplicativo estiver instalado.
/ALIAS:<alias da tarefa>	Esta chave permite atribuir um nome temporário à tarefa que pode ser usado para acessar a tarefa durante sua execução. Por exemplo, é possível exibir estatísticas da tarefa usando o comando TASK. O alias da tarefa deve ser exclusivo entre os aliases de tarefas de todos os componentes funcionais do Kaspersky Embedded Systems Security 2.2. Se esta chave não for especificada, será usada update_<kavshell_pid>, por exemplo, update_1234. No Console do Aplicativo, a tarefa será atribuída automaticamente Update-databases (<data hora>), por exemplo, Update-databases 16/08/2007 17h41m02.
/W:<caminho do arquivo de log de tarefas>	Se esta chave for especificada, o Kaspersky Embedded Systems Security 2.2 salvará o arquivo de log de tarefas com o nome definido pelo valor da chave. O arquivo de log contém estatísticas de execução da tarefa, a hora em que ela foi iniciada e concluída (interrompida), além de informações sobre os eventos da tarefa. O log é usado para registrar eventos definidos pelas configurações de log de tarefas e pelo log de eventos do Kaspersky Embedded Systems Security 2.2 no "Visualizador de Eventos". É possível especificar o caminho absoluto ou relativo do arquivo de log. Se for especificado apenas o nome do arquivo sem seu caminho, o arquivo de log será criado na pasta atual. Ao reiniciar o comando com as mesmas configurações de log, o arquivo de log existente será substituído. O arquivo de log pode ser exibido enquanto uma tarefa está em execução. O log é exibido no nó **Logs de tarefa** do Console do Aplicativo. Se o Kaspersky Embedded Systems Security 2.2 não conseguir criar o arquivo de log, ele não interromperá a execução do comando ou exibirá uma mensagem de erro.

Códigos de retorno do comando KAVSHELL UPDATE (na página 254).

Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security 2.2. KAVSHELL ROLLBACK

O comando `KAVSHELL ROLLBACK` pode ser usado para executar uma tarefa do sistema de Reversão do banco de dados do Kaspersky Embedded Systems Security 2.2 (reversão dos bancos de dados do Kaspersky Embedded Systems Security 2.2 para a versão instalada anteriormente). O comando é executado de forma síncrona.

Sintaxe do comando:

```
KAVSHELL ROLLBACK
```

Códigos de retorno do comando KAVSHELL ROLLBACK (na página 255).

Gerenciando inspeção do log KAVSHELL TASK LOG-INSPECTOR

O comando `KAVSHELL TASK LOG-INSPECTOR` pode ser usado para monitorar a integridade do ambiente com base na análise do Log de Eventos do Windows.

Sintaxe do comando

```
KAVSHELL TASK LOG-INSPECTOR
```

Exemplos do comando

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Tabela 48. Modificadores do comando KAVSHELL TASK LOG-INSPECTOR

Chave	Descrição
/START	Inicia a tarefa especificada no modo assíncrono.
/STOP	Interrompe a tarefa especificada.
/STATE	Retorna o status da tarefa atual (por exemplo, *Executando*, Concluída, Pausada, Interrompida, Falhou, Iniciando, Recuperando).
/STATISTICS	Obtém as estatísticas da tarefa - informações sobre o número de objetos processados a partir da hora de início da tarefa até agora.

Códigos de retorno do comando KAVSHELL TASK LOG-INSPECTOR (consulte a seção "Códigos de retorno do comando KAVSHELL TASK LOG-INSPECTOR" na página 253).

Ativando o aplicativo KAVSHELL LICENSE

As chaves do Kaspersky Embedded Systems Security 2.2 e os códigos de ativação podem ser gerenciados usando o comando `KAVSHELL LICENSE`.

> A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL FULLSCAN

```
KAVSHELL LICENSE [/ADD:<arquivo de chave | código de ativação> [/R] | /DEL:<chave
```

```
| número do código de ativação>]
```

Exemplos do comando KAVSHELL SCAN

► *Para ativar o aplicativo, execute o comando:*

```
KAVSHELL.EXE LICENSE / ADD: <chave ou código de ativação>
```

► *Para visualizar informações sobre chaves adicionadas, execute o comando:*

```
KAVSHELL LICENSE
```

► *Para remover uma chave adicionada com o número 0000-000000-00000001, execute o comando:*

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

O comando `KAVSHELL LICENSE` pode ser executado com ou sem chaves (veja a tabela abaixo).

Tabela 49. Chaves do comando KAVSHELL LICENSE

Chave	Descrição
Sem chaves	O comando retorna as seguintes informações sobre chaves adicionadas: • Chave. • Tipo de licença (comercial). • Duração da licença associada à chave. • Status da chave (ativa ou adicional). Se o valor especificado for *, a chave foi adicionada como uma chave adicional.
/ADD: <nome do arquivo de chave ou código de ativação>	Adiciona a chave através do arquivo ou código de ativação especificado. As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho de um arquivo de chave; não são permitidas variáveis do ambiente do usuário.
/R	O código ou chave de ativação /R é uma adição ao código ou chave de ativação /ADD e indica que o código de ativação ou a chave que está sendo adicionado é um código ou chave de ativação adicional.
/DEL: <chave ou código de ativação>	Exclui a chave com o número especificado ou o código de ativação selecionado.

Os códigos de retorno do comando KAVSHELL LICENSE (consulte a seção "Códigos de retorno do comando KAVSHELL LICENSE" na página 255).

Ativando, configurando e desativando o log de rastreamento. KAVSHELL TRACE

O comando `KAVSHELL TRACE` pode ser usado para ativar o log de rastreamento para todos os subsistemas do Kaspersky Embedded Systems Security 2.2 e para configurar o nível de detalhe do log.

> O Kaspersky Embedded Systems Security 2.2 grava as informações nos arquivos de rastreamento e no arquivo de despejo de modo não criptografado.

Sintaxe de comando de KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<caminho da pasta do arquivo de log de rastreamento>
[/S:<tamanho máximo do log em megabytes>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Se o log de rastreamento for mantido e você desejar alterar suas configurações, insira o comando `KAVSHELL TRACE` com a chave /ON e especifique as configurações do log com os valores das chaves /S e /LVL (veja a tabela abaixo).

Tabela 50. Chaves do comando KAVSHELL TRACE

Chave	Descrição
/ON	Ativa o log de rastreamento.
/F:<pasta com arquivos do log de rastreamento>	Esta chave especifica o caminho completo da pasta na qual os arquivos do log de rastreamento serão salvos (obrigatório). Se for especificado o caminho de uma pasta não existente, não será criado log de rastreamento. É possível usar caminhos de rede em formato UNC (Universal Naming Convention), mas não podem ser especificados caminhos de pastas em unidades de rede do computador protegido. Se um caractere de espaço for incluído no nome de uma pasta na qual você especifica o caminho como o valor da chave, coloque o caminho dessa pasta entre aspas, por exemplo: /F:"C\Trace Folder". As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho dos arquivos de log de rastreamento; não são permitidas variáveis do ambiente do usuário.
/S: <tamanho máximo do arquivo de log em megabytes>	Esta chave define o tamanho máximo de um único arquivo de log de rastreamento. Assim que o arquivo de log atingir o nível máximo, o Kaspersky Embedded Systems Security 2.2 começará a gravar informações em um novo arquivo; o arquivo de log anterior será salvo. Se o valor desta chave não for especificado, o tamanho máximo de um arquivo de log será 50 MB.
/LVL:debug|info|warning|error|critical	Esta chave configura o nível de detalhe do log, desde o valor máximo (**Todas as informações da depuração**) no qual todos os eventos são registrados no log, até o valor mínimo (**Eventos críticos**), no qual somente os eventos críticos são registrados. Se esta chave não for especificada, os eventos com o nível de detalhamento **Todas as informações da depuração** serão registrados no log de rastreamento.
/OFF	Esta chave desativa o log de rastreamento.

Exemplos do comando KAVSHELL TRACE

- *Para ativar o log de rastreamento usando o nível de detalhamento **Todas as informações da depuração** e o tamanho máximo de log de 200 MB, e salvar o arquivo de log na pasta C:\Pasta de Rastreamento, execute o comando:*

```
KAVSHELL TRACE /ON /F:"C:\Pasta de Rastreamento" /S:200
```

- *Para ativar o log de rastreamento usando o nível de detalhamento **Eventos importantes** e salvar o arquivo de log na pasta C:\Pasta de Rastreamento, execute o comando:*

```
KAVSHELL TRACE /ON /F:"C:\Pasta de Rastreamento" /LVL:warning
```

- *Para desativar o log de rastreamento:*

```
KAVSHELL TRACE /OFF
```

Códigos de retorno do comando KAVSHELL TRACE (consulte a seção "Códigos de retorno do comando KAVSHELL TRACE" na página 255).

Desfragmentação de arquivos de log do Kaspersky Embedded Systems Security 2.2. KAVSHELL VACUUM

Usando o comando `KAVSHELL VACUUM` você pode desfragmentar os arquivos de log do aplicativo. Ele permite evitar erros de sistema ou erros durante o trabalho do Kaspersky Embedded Systems Security 2.2 conectados a um armazenamento rígido de log.

> A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Recomenda-se aplicar o comando `KAVSHELL VACUUM` para otimizar o armazenamento de arquivos de log no caso de inicializações frequentes de tarefas de Verificação por Demanda e de atualização. Ao executar o comando, o Kaspersky Embedded Systems Security 2.2 renova uma estrutura lógica dos arquivos de log do aplicativo armazenados em um computador protegido pelo caminho especificado.

Por padrão, os arquivos de log do aplicativo são armazenados em C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\2.2\Reports. Se você tiver especificado manualmente outro caminho de armazenamento de log, o comando `KAVSHELL VACUUM` realizará a desfragmentação de arquivos na pasta que é especificada nas configurações de log do Kaspersky Embedded Systems Security 2.2.

> O tamanho grande de arquivos em desfragmentação aumenta o período de execução do comando `KAVSHELL VACUUM`.

> As tarefas de Proteção em Tempo Real e de Controle do Computador não estão disponíveis para serem executadas durante a execução do comando `KAVSHELL VACUUM`. O processo de desfragmentação em andamento restringe o acesso ao log do Kaspersky Embedded Systems Security 2.2 e rejeita o registro de eventos em log. Para evitar a redução do nível de segurança, recomenda-se planejar com antecedência a execução do comando `KAVSHELL VACUUM` para um período de inatividade.

► *Para desfragmentar os arquivos de log do Kaspersky Embedded Systems Security 2.2, execute o seguinte comando:*

```
KAVSHELL VACUUM
```

A execução do comando é possível se iniciada com direitos de conta do administrador local.

Limpando a base iSwift. KAVSHELL FBRESET

O Kaspersky Embedded Systems Security 2.2 usa a tecnologia iSwift que permite que o aplicativo evite verificar novamente arquivos que não foram modificados desde a última verificação (**Usar a tecnologia iSwift**).

O Kaspersky Embedded Systems Security 2.2 cria os arquivos klamfb.dat e klamfb2.dat no diretório de informações de volume %SYSTEMDRIVE%\System, contendo informações sobre os objetos limpos que já foram verificados. O arquivo klamfb.dat (klamfb2.dat) cresce com o número de arquivos verificados pelo Kaspersky Embedded Systems Security 2.2. O arquivo contém somente informações atuais sobre arquivos existentes no sistema: se um arquivo for removido, o Kaspersky Embedded Systems Security 2.2 eliminará as informações sobre ele do klamfb.dat.

Para limpar um arquivo, use o comando `KAVSHELL FBRESET`.

Lembre-se sempre das seguintes instruções de operação do comando `KAVSHELL FBRESET`:

- Ao limpar o arquivo klamfb.dat por meio do comando KAVSHELL FBRESET, o Kaspersky Embedded Systems Security 2.2 não pausa a proteção (ao contrário dos casos de exclusão manual de klamfb.dat).
- O Kaspersky Embedded Systems Security 2.2 poderá aumentar a carga de trabalho do computador após os dados serem limpos no klamfb.dat. Nesse caso, o Antivírus verifica todos os arquivos acessados pela primeira vez desde a limpeza de klamfb.dat. Após a verificação, o Kaspersky Embedded Systems Security 2.2 adiciona novamente ao arquivo klamfb.dat as informações sobre cada objeto verificado. No caso de novas tentativas de acessar o objeto, a tecnologia iSwift evitará que o arquivo seja verificado novamente, desde que ele permaneça inalterado.

A execução do comando `KAVSHELL FBRESET` está disponível apenas se a linha de comando for iniciada na conta SYSTEM.

Ativando e desativando a criação do arquivo de despejo. KAVSHELL DUMP

A criação de instantâneos (arquivo de despejo) para processos do Kaspersky Embedded Systems Security 2.2 em casos de encerramento anormal de processos pode ser ativada ou desativada usando o comando `KAVSHELL DUMP` (consulte a tabela abaixo). É possível obter instantâneos adicionais da memória dos processos do Kaspersky Embedded Systems Security 2.2 em andamento a qualquer momento.

Para que o arquivo de despejo seja criado com sucesso, o comando `KAVSHELL DUMP` deve ser executado na conta do sistema local (SYSTEM).

Sintaxe de comando para KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<pasta com o arquivo de despejo>|/SNAPSHOT /F:< pasta
com o arquivo de despejo> / P:<pid> | /OFF>
```

Exemplos do comando KAVSHELL DUMP

► *Para ativar a criação do arquivo de despejo e salvá-lo na pasta C:\Pasta de Despejo, execute o comando:*

```
KAVSHELL DUMP /ON /F:"C:\Pasta de Despejo"
```

► *Para obter um despejo para o processo com ID 1234 na pasta C:/Despejos, execute o comando:*

```
KAVSHELL DUMP /SNAPSHOT /F: C:\Dumps /P:1234
```

► *Para desativar a geração do arquivo de despejo, execute o comando:*

```
KAVSHELL DUMP /OFF
```

Tabela 51. Chaves do comando KAVSHELL DUMP

Chave	Descrição
/ON	Ativa a criação do arquivo de despejo de memória do processo em casos de encerramento anormal.
/F:<caminho da pasta com arquivos de despejo>	Esta é uma chave obrigatória. Ela especifica o caminho da pasta na qual o arquivo de despejo será salvo. Se for especificado o caminho de uma pasta não existente, não será criado o arquivo de despejo. É possível usar caminhos de rede em formato UNC (Universal Naming Convention), mas não podem ser especificados caminhos de pastas em unidades de rede do computador protegido. As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho da pasta com o arquivo de despejo da memória; não são permitidas variáveis do ambiente do usuário.
/SNAPSHOT	Obtenha um instantâneo da memória do processo especificado do Kaspersky Embedded Systems Security 2.2 em andamento e salva o arquivo de despejo na pasta cujo caminho é especificado pela chave /F.
/P	O identificador do processo, PID, é exibido no Gerenciador de Tarefas do Microsoft Windows.
/OFF	Desativa a criação arquivo de despejo de memória do processo em casos de encerramento anormal.

Códigos de retorno do comando KAVSHELL DUMP (consulte a seção "Códigos de retorno do comando KAVSHELL DUMP" na página 256).

Importando configurações. KAVSHELL IMPORT

O comando `KAVSHELL IMPORT` permite importar as configurações do Kaspersky Embedded Systems Security 2.2, suas funções e tarefas a partir de um arquivo de configuração para uma cópia do Kaspersky Embedded

Systems Security 2.2 no computador protegido. É possível criar um arquivo de configuração usando o comando `KAVSHELL EXPORT`.

> A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe de comando de KAVSHELL IMPORT

`KAVSHELL IMPORT <nome do arquivo de configuração e caminho do arquivo>`

Exemplos do comando KAVSHELL IMPORT

`KAVSHELL IMPORT Host1.xml`

Tabela 52. Chaves do comando KAVSHELL IMPORT

Chave	Descrição
<nome do arquivo de configuração e caminho do arquivo>	Nome do arquivo de configuração usado como fonte de importação das configurações. As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho do arquivo; não são permitidas variáveis do ambiente do usuário.

Códigos de retorno do comando KAVSHELL IMPORT (consulte a seção "Códigos de retorno do comando KAVSHELL IMPORT" na página 257).

Exportando configurações. KAVSHELL EXPORT

O comando `KAVSHELL EXPORT` permite exportar todas as configurações do Kaspersky Embedded Systems Security 2.2 e suas tarefas atuais para um arquivo de configuração, para depois importá-las para cópias do Kaspersky Embedded Systems Security 2.2 instaladas em outros computadores.

Sintaxe de comando de KAVSHELL EXPORT

`KAVSHELL EXPORT <nome do arquivo de configuração e caminho do arquivo>`

Exemplos do comando KAVSHELL EXPORT

`KAVSHELL EXPORT Host1.xml`

Tabela 53. Chaves do comando KAVSHELL EXPORT

Chave	Descrição
<nome do arquivo de configuração e caminho do arquivo>	Nome do arquivo de configuração que conterá as configurações. É possível atribuir qualquer extensão ao arquivo de configuração. As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho do arquivo; não são permitidas variáveis do ambiente do usuário.

Códigos de retorno do comando KAVSHELL EXPORT (consulte a seção "Códigos de retorno do comando KAVSHELL EXPORT" na página 257).

Integração com Microsoft Operations Management Suite. KAVSHELL OMSINFO

Usando o comando KAVSHELL OMSINFO, é possível revisar o status do aplicativo e informações sobre ameaças detectadas por bancos de dados de antivírus e pelo serviço da KSN. Os dados sobre ameaças são tomados dos logs de evento disponíveis.

Sintaxe do comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <caminho completo para arquivo gerado com nome do arquivo>
```

Exemplos do comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Tabela 54. Chaves do comando KAVSHELL OMSINFO

Chave	Descrição
<caminho do arquivo gerado com nome de arquivo>	Nome do arquivo gerado que conterá informações sobre status de aplicativo e ameaças detectadas.

Códigos de retorno da linha de comando

Nesta seção

Código de retorno dos comandos KAVSHELL START e KAVSHELL STOP

Tabela 55. Código de retorno dos comandos KAVSHELL START e KAVSHELL STOP

Código de retorno	Descrição
0	Operação concluída com êxito
-3	Erro de permissões
-5	Sintaxe de comando inválida
-6	Operação inválida (por exemplo, o serviço do Kaspersky Embedded Systems Security 2.2 já está em execução ou já foi interrompido)
-7	Serviço não registrado
-8	A inicialização de Serviço automático está desativada.
-9	A tentativa de iniciar o computador em outra conta de usuário falhou (por padrão, o serviço do Kaspersky Embedded Systems Security 2.2 é executado na conta de usuário do Sistema local)
-99	Erro desconhecido

Código de retorno dos comandos KAVSHELL SCAN e KAVSHELL SCANCRITICAL

Tabela 56. Código de retorno dos comandos KAVSHELL SCAN e KAVSHELL SCANCRITICAL

Código de retorno	Descrição
0	Operação concluída com êxito (nenhuma ameaça detectada)
1	Operação cancelada
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (arquivo com a lista de escopos da verificação não encontrado)
-5	Sintaxe de comando inválida ou escopo da verificação não definida
-80	Objetos infectados e outros detectados
-81	Objetos possivelmente infectados detectados
-82	Erros de processamento detectados
-83	Objetos não verificados detectados
-84	Objetos corrompidos detectados
-85	Falha ao criar o arquivo de log de tarefas

Código de retorno	Descrição
-99	Erro desconhecido
-301	Chave inválida

Códigos de retorno do comando KAVSHELL TASK LOG-INSPECTOR

Tabela 57. Código de retorno do comando KAVSHELL TASK LOG-INSPECTOR

Código de retorno	Descrição
0	Operação concluída com êxito
-6	Operação inválida (por exemplo, o serviço do Kaspersky Embedded Systems Security 2.2 já está em execução ou já foi interrompido)
402	Tarefa já sendo executada (para modificador /STATE)

Códigos de retorno do comando KAVSHELL TASK

Tabela 58. Códigos de retorno do comando KAVSHELL TASK

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (tarefa não encontrada)
-5	Sintaxe de comando inválida
-6	Operação inválida (por exemplo, tarefa não está em execução, já em execução ou que não pode ser pausada)
-99	Erro desconhecido
-301	Chave inválida
401	Tarefa não sendo executada (para modificador /STATE)
402	Tarefa já sendo executada (para modificador /STATE)
403	Tarefa já pausada (para modificador /STATE)
-404	Erro ao executar a operação (a alteração no status da tarefa causou sua falha)

Códigos de retorno do comando KAVSHELL RTP

Tabela 59. Códigos de retorno do comando KAVSHELL RTP

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (uma das tarefas de proteção em tempo real ou todas as tarefas de proteção em tempo real não encontradas)
-5	Sintaxe de comando inválida
-6	Operação inválida (por exemplo, a tarefa já está em execução ou já foi interrompida)
-99	Erro desconhecido
-301	Chave inválida

Códigos de retorno do comando KAVSHELL UPDATE

Tabela 60. Códigos de retorno do comando KAVSHELL UPDATE

Código de retorno	Descrição
0	Operação concluída com êxito
200	Todos os objetos estão atualizados (os bancos de dados ou componentes do programa estão atualizados)
-2	Serviço não está em execução
-3	Erro de permissões
-5	Sintaxe de comando inválida
-99	Erro desconhecido
-206	Os arquivos de extensão estão ausentes da fonte especificada ou têm um formato desconhecido
-209	Erro ao conectar à fonte de atualização
-232	Erro de autenticação ao conectar ao servidor proxy
-234	Erro ao conectar o Kaspersky Security Center
-235	O Kaspersky Embedded Systems Security 2.2 não foi autenticado ao conectar à fonte de atualização
-236	O banco de dados do aplicativo está corrompido
-301	Chave inválida

Códigos de retorno do comando KAVSHELL ROLLBACK

Tabela 61. Códigos de retorno do comando KAVSHELL ROLLBACK

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-99	Erro desconhecido
-221	Cópia de backup do banco de dados não encontrada ou corrompida
-222	Cópia de backup do banco de dados corrompida

Códigos de retorno do comando KAVSHELL LICENSE

Tabela 62. Códigos de retorno do comando KAVSHELL LICENSE

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Privilégios insuficientes para gerenciar chaves
-4	Chave com o número especificado não encontrada
-5	Sintaxe de comando inválida
-6	Operação inválida (chave já adicionada)
-99	Erro desconhecido
-301	Chave inválida
-303	A licença aplica-se a um aplicativo diferente

Códigos de retorno do comando KAVSHELL TRACE

Tabela 63. Códigos de retorno do comando KAVSHELL TRACE

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões

Código de retorno	Descrição
-4	Objeto não encontrado (caminho especificado como caminho para a pasta de logs de rastreamento não encontrado)
-5	Sintaxe de comando inválida
-6	Operação inválida (tentativa de execução do comando KAVSHELL TRACE /OFF se a criação de log de despejo já estiver desativada)
-99	Erro desconhecido

Códigos de retorno do comando KAVSHELL FBRESET

Tabela 64. Códigos de retorno do comando KAVSHELL FBRESET

Código de retorno	Descrição
0	Operação concluída com êxito
-99	Erro desconhecido

Códigos de retorno do comando KAVSHELL DUMP

Tabela 65. Códigos de retorno do comando KAVSHELL DUMP

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (caminho especificado como caminho para a pasta do arquivo de despejo não encontrado; processo com PID especificado não encontrado)
-5	Sintaxe de comando inválida
-6	Operação inválida (tentativa de execução do comando KAVSHELL DUMP/OFF se a criação de arquivo de despejo já estiver desativada)
-99	Erro desconhecido

Códigos de retorno do comando KAVSHELL IMPORT

Tabela 66. Códigos de retorno do comando KAVSHELL IMPORT

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (arquivo de configuração importável não encontrado)
-5	Sintaxe inválida
-99	Erro desconhecido
501	Operação concluída com êxito, no entanto ocorreu um erro/comentário durante a execução do comando, por exemplo, o Kaspersky Embedded Systems Security 2.2 não importou parâmetros de algum componente funcional
-502	O arquivo sendo importando está ausente ou tem um formato não reconhecido
-503	Configurações incompatíveis (arquivo de configuração exportado a partir de um programa diferente ou de uma versão posterior e incompatível do Kaspersky Embedded Systems Security 2.2)

Códigos de retorno do comando KAVSHELL EXPORT

Tabela 67. Códigos de retorno do comando KAVSHELL EXPORT

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-5	Sintaxe inválida
-10	Não foi possível criar um arquivo de configuração (por exemplo, não existe acesso à pasta especificada no caminho para o arquivo)
-99	Erro desconhecido
501	Operação concluída com êxito, no entanto ocorreu um erro/comentário durante a execução do comando, por exemplo, o Kaspersky Embedded Systems Security 2.2 não exportou parâmetros de algum componente funcional

Integração com sistemas de terceiros

Esta seção descreve a integração do Kaspersky Embedded Systems Security 2.2 com recursos e tecnologias de terceiros.

Neste capítulo

Monitoramento do desempenho. Contadores do Kaspersky Embedded Systems Security 2.2

Esta seção fornece informações sobre os contadores do Kaspersky Embedded Systems Security 2.2: contadores de desempenho do Monitor do Sistema e contadores e interceptações SNMP.

Neste capítulo

Contadores de desempenho do Monitor do Sistema

Esta seção contém informações sobre os contadores de desempenho do Monitor do Sistema do Microsoft Windows, registrados pelo Kaspersky Embedded Systems Security 2.2 durante a instalação.

Nesta seção

Sobre os contadores SNMP do Kaspersky Embedded Systems Security 2.2

O componente **Contadores de desempenho** está incluído nos componentes instalados do Kaspersky Embedded Systems Security 2.2 por padrão. O Kaspersky Embedded Systems Security 2.2 registra os seus próprios contadores de desempenho para o Monitor do Sistema do Microsoft Windows durante a instalação.

Usando os contadores do Kaspersky Embedded Systems Security 2.2, você pode controlar o desempenho do aplicativo enquanto as tarefas de Proteção em tempo real são executadas. Você pode identificar locais problemáticos durante a execução com outros aplicativos e falhas de recursos. Você pode diagnosticar configurações indesejáveis e travamentos do Kaspersky Embedded Systems Security 2.2 durante a operação.

Você pode visualizar os contadores de desempenho do Kaspersky Embedded Systems Security 2.2 abrindo o console **Desempenho** no item **Administração** do Painel de Controle do Windows.

As seções a seguir listam as definições dos contadores, os intervalos recomendados para as leituras, os valores limite e recomendações de configurações do Kaspersky Embedded Systems Security 2.2 caso os valores dos contadores os excedam.

Número total de solicitações negadas

Tabela 68. Número total de solicitações negadas

Nome	Número total de solicitações negadas
Definição	Número total de solicitações do driver de interceptação de arquivos para processar os objetos que não foram aceitos por processos do aplicativo; contado a partir do momento em que o Kaspersky Embedded Systems Security 2.2 foi iniciado pela última vez. O aplicativo ignora objetos para os quais as solicitações para processamento são negadas pelos processos do Kaspersky Embedded Systems Security 2.2.
Finalidade	Este contador pode ajudá-lo a detectar: • Quedas de qualidade na Proteção em Tempo Real que afetam os processos de trabalho do Kaspersky Embedded Systems Security 2.2. • Interrupção da proteção em tempo real devido a falhas de triagem da interceptação de arquivos.
Valor normal / limite	0 / 1.
Intervalo de leitura recomendado	1 hora.

Recomendações de configuração caso o valor exceda o limite	O número de solicitações para objetos com processamento negado corresponde ao número de objetos ignorados. As situações que se seguem são possíveis, dependendo do comportamento do contador: • O contador mostra várias solicitações negadas durante um período prolongado de tempo: todos os processos do Kaspersky Embedded Systems Security 2.2 são totalmente carregados, portanto, o Kaspersky Embedded Systems Security 2.2 não pode verificar objetos. Para evitar ignorar objetos, aumente o número de processos do aplicativo para as tarefas de Proteção em tempo real. Você pode usar essas configurações do Kaspersky Embedded Systems Security 2.2 como **Número máximo de processos ativos** e **Número de processos para a Proteção em Tempo Real**. • O número de solicitações recusadas excede de forma significativa o limite crítico e continua crescendo rapidamente: a interceptação travou. O Kaspersky Embedded Systems Security 2.2 não está verificando os objetos ao acessar. Reinicie o Kaspersky Embedded Systems Security 2.2.

Número total de solicitações ignoradas

Tabela 69. Número total de solicitações ignoradas

Nome	Número total de solicitações ignoradas
Definição	O número total de pedidos do driver de interceptação de arquivos para processar objetos recebidos pelo Kaspersky Embedded Systems Security 2.2, mas que não geraram eventos de conclusão de processamento; esse número é contado a partir do momento em que o aplicativo foi iniciado pela última vez. Se um pedido de processamento de um objeto desse tipo aceito por um dos processos de trabalho não enviar um evento para conclusão do processamento, o driver irá transferir esse pedido para outro processo e o valor do contador **Número total de pedidos ignorados** irá aumentar em 1. Se o driver tiver percorrido todos os processos de trabalho e nenhum deles tiver recebido o pedido de processamento (por estar ocupado) ou enviado eventos para conclusão do processamento, o Kaspersky Embedded Systems Security 2.2 ignorará esse objeto, pelo que o valor do contador **Número total de pedidos ignorados** irá aumentar em 1.
Finalidade	Esse contador permite detectar quebras no desempenho devido a falhas na interceptação.
Valor normal / limite	0 / 1
Intervalo de leitura recomendado	1 hora
Recomendações de configuração caso o valor exceda o limite	Se o valor do contador for diferente de zero, um ou vários fluxos de triagem de interceptação de arquivos foram congelados e estão inativos. O valor do contador corresponde ao número de fluxos atualmente inativos. Se a velocidade de verificação não for satisfatória, reinicie o Kaspersky Embedded Systems Security 2.2 para restaurar os fluxos offline.

Número de solicitações não processadas devido à falta de recursos do sistema

Tabela 70. Número de solicitações não processadas devido à falta de recursos do sistema

Nome	Número de solicitações não processadas devido à falta de recursos.
Definição	Número total de solicitações do driver de interceptação de arquivos que não foram processados devido à falta de recursos do sistema (por exemplo, de RAM); contado a partir do momento em que o Kaspersky Embedded Systems Security 2.2 foi iniciado pela última vez. O Kaspersky Embedded Systems Security 2.2 ignora solicitações de objetos para processar que não sejam processados pelo driver de interceptação de arquivos.
Finalidade	Esse contador pode ser usado para detectar e eliminar qualidade potencialmente baixa na proteção em tempo real que ocorre devido a um volume reduzido nos recursos do sistema.
Valor normal / limite	0 / 1.
Intervalo de leitura recomendado	1 hora.
Recomendações de configuração caso o valor exceda o limite	Se o valor do contador for diferente de zero, os processos de trabalho do Kaspersky Embedded Systems Security 2.2 precisam de mais RAM para processar solicitações. Talvez os processos ativos de outros aplicativos estejam usando toda a RAM disponível.

Número de solicitações enviadas para serem processadas

Tabela 71. Número de solicitações enviadas para serem processadas

Nome	Número de solicitações enviadas para serem processadas.
Definição	O número de objetos que aguardam processamento pelos processos em execução.
Finalidade	Este contador pode ser usado para rastrear a carga nos processos de trabalho do Kaspersky Embedded Systems Security 2.2 e o nível geral de atividade de arquivos no computador.
Valor normal / limite	O valor do contador pode variar de acordo com o nível de atividade de arquivos do computador.
Intervalo de leitura recomendado	1 minuto
Recomendações de configuração caso o valor exceda o limite	Não

Número médio de fluxos de triagem de interceptação de arquivos

Tabela 72. Número médio de fluxos de triagem de interceptação de arquivos

Nome	Número médio de fluxos de triagem de interceptação de arquivos.
Definição	O número de fluxos de triagem de interceptação de arquivos em um processo e a média de todos os processos envolvidos no momento em tarefas de proteção em tempo real.
Finalidade	Esse contador pode ser usado para detectar e eliminar a baixa qualidade que ocorra na proteção em tempo real devido a carga completa nos processos do Kaspersky Embedded Systems Security 2.2.
Valor normal / limite	Varia / 40
Intervalo de leitura recomendado	1 minuto
Recomendações de configuração caso o valor exceda o limite	É possível criar até 60 fluxos de triagem de interceptação de arquivos em cada processo de trabalho. Se o valor do contador se aproximar de 60, haverá o risco de que nenhum dos processos de trabalho possa processar a próxima solicitação da fila a partir do driver de interceptação de arquivos e que o Kaspersky Embedded Systems Security 2.2 ignore o objeto. Aumente o número de processos do Kaspersky Embedded Systems Security 2.2 para tarefas de proteção em tempo real. Você pode usar essas configurações do Kaspersky Embedded Systems Security 2.2 como **Número máximo de processos ativos** e **Número de processos para a Proteção em Tempo Real**.

Número máximo de fluxos de triagem de interceptação de arquivos

Tabela 73. Número máximo de fluxos de triagem de interceptação de arquivos

Nome	Número máximo de fluxos de triagem de interceptação de arquivos.
Definição	O número de fluxos de triagem de interceptação de arquivos em um processo e o máximo de todos os processos envolvidos no momento em tarefas de proteção em tempo real.
Finalidade	Esse contador permite detectar e eliminar quebras no desempenho devido a uma distribuição desequilibrada das cargas nos processos em execução.
Valor normal / limite	Varia / 40
Intervalo de leitura recomendado	1 minuto
Recomendações de configuração caso o valor exceda o limite	Se o valor desse contador exceder de forma significativa e contínua o valor do contador **Número médio de fluxos de interceptação de arquivos**, o Kaspersky Embedded Systems Security 2.2 está distribuindo a carga de forma desequilibrada pelos processos em execução. Reinicie o Kaspersky Embedded Systems Security 2.2.

Número de elementos na fila de objetos infectados

Tabela 74. Número de elementos na fila de objetos infectados

Nome	Número de itens na fila de objetos infectados.
Definição	Número de objetos infectados atualmente aguardando processamento (desinfecção ou exclusão).
Finalidade	Este contador pode ajudá-lo a detectar: • Interrupção da Proteção em Tempo Real devido a possíveis falhas de triagem da interceptação de arquivos. • Sobrecarga de processos devido à distribuição não uniforme do tempo do processador entre diferentes processos de trabalho e o Kaspersky Embedded Systems Security 2.2. • Surtos de vírus.
Valor normal / limite	Este valor pode ser diferente de zero enquanto o Kaspersky Embedded Systems Security 2.2 está processando objetos infectados ou possivelmente infectados, mas retornará a zero após a conclusão do processamento / O valor permanece como diferente de zero durante um período de tempo prolongado.
Intervalo de leitura recomendado	1 minuto
Recomendações de configuração caso o valor exceda o limite	Se o valor do contador não retornar a zero durante um período de tempo prolongado: • O Kaspersky Embedded Systems Security 2.2 não está processando objetos (talvez a triagem de interceptação de arquivos tenha travado). Reinicie o Kaspersky Embedded Systems Security 2.2. • Não existe tempo de processador suficiente para processar os objetos. Certifique-se de que o Kaspersky Embedded Systems Security 2.2 obtenha tempo de processador adicional (por exemplo, reduzindo a carga de outros aplicativos no computador). • Ocorreu um surto de vírus. Um número muito elevado de objetos infectados ou possivelmente infectados na tarefa Proteção de Arquivos em Tempo Real é também um sinal de um surto de vírus. Você pode exibir informações sobre o número de objetos detectados nas estatísticas ou logs de tarefas.

Número de objetos processados por segundo

Tabela 75. Número de objetos processados por segundo

Nome	Número de objetos processados por segundo.
Definição	Número de objetos processados, dividido pelo tempo necessário para processar esses objetos (calculado em intervalos de tempo idênticos).

Finalidade	Este contador reflete a velocidade do processamento de objetos; ele pode ser usado para detectar e eliminar pontos baixos no desempenho do computador que ocorrem devido a atribuição de tempo de processador insuficiente aos processos do Kaspersky Embedded Systems Security 2.2 ou erros na operação do Kaspersky Embedded Systems Security 2.2.
Valor normal / limite	Varia / N.º
Intervalo de leitura recomendado	1 minuto.
Recomendações de configuração caso o valor exceda o limite	Os valores deste contador dependem dos valores definidos nas configurações do Kaspersky Embedded Systems Security 2.2 e da carga no computador de processos de outros aplicativos. Observe o nível médio dos valores do contador por um longo período. Se o nível geral dos valores do contador diminuir, é possível uma das seguintes situações: • Os processos do Kaspersky Embedded Systems Security 2.2 não têm tempo de processador suficiente para processar os objetos. Certifique-se de que o Kaspersky Embedded Systems Security 2.2 obtenha tempo de processador adicional (por exemplo, reduzindo a carga de outros aplicativos no computador). • Ocorreu um erro no Kaspersky Embedded Systems Security 2.2 (vários fluxos estão ociosos). Reinicie o Kaspersky Embedded Systems Security 2.2.

Contadores e interceptações SNMP do Kaspersky Embedded Systems Security 2.2

Esta seção contém informações sobre os contadores e interceptações do Kaspersky Embedded Systems Security 2.2.

Nesta seção

Sobre contadores e interceptações SNMP do Kaspersky Embedded Systems Security 2.2

Se você tiver incluído **Contadores e interceptações SNMP** no conjunto de componentes do Antivírus a ser instalado, você poderá visualizar os contadores e interceptações do Kaspersky Embedded Systems Security 2.2 usando o protocolo Simple Network Management Protocol (SNMP).

Para exibir os contadores e as interceptações do Kaspersky Embedded Systems Security 2.2 da estação de trabalho do administrador, inicie o Serviço SNMP no computador protegido e os Serviços SNMP e de Interceptação SNMP na estação de trabalho do administrador.

Contadores SNMP do Kaspersky Embedded Systems Security 2.2

Esta seção contém tabelas com uma descrição das configurações para os contadores SNMP do Kaspersky Embedded Systems Security 2.2.

Nesta seção

Contadores de desempenho

Tabela 76. Contadores de desempenho

Contador	Definição
currentRequestsAmount	Número de solicitações enviadas para serem processadas. (na página 261)
currentInfectedQueueLength	Número de elementos na fila de objetos infectados (consulte a seção "Número de elementos na fila de objetos infectados" na página 263)
currentObjectProcessingRate	Número de objetos processados por segundo (na página 263)
currentWorkProcessesNumber	Número atual de processos de trabalho usados pelo Kaspersky Embedded Systems Security 2.2

Contadores de Quarentena

Tabela 77. Contadores de Quarentena

Contador	Definição
totalObjects	Número de objetos atualmente na Quarentena
totalSuspiciousObjects	Número de objetos possivelmente infectados atualmente na Quarentena
currentStorageSize	Tamanho total dos dados na Quarentena (MB)

Contadores de Backup

Tabela 78. Contadores de Backup

Contador	Definição
currentBackupStorageSize	Tamanho total dos dados no Backup (MB)

Contadores gerais

Tabela 79. Contadores gerais

Contador	Definição
lastCriticalAreasScanAge	O período desde a última verificação completa das áreas críticas do computador (tempo decorrido em segundos desde a conclusão da última tarefa de *Verificação de áreas críticas*).
licenseExpirationDate	Data de expiração da licença se uma chave ativa ou chaves adicionais tiverem sido adicionadas, a data de expiração da licença associada à chave adicional é exibida.
currentApplicationUptime	O tempo de execução do Kaspersky Embedded Systems Security 2.2 desde que foi iniciado pela última vez, em centésimos de segundos.
currentFileMonitorTaskStatus	Status da tarefa de Proteção de Arquivos em Tempo Real: **Ativada** – em execução; **Desativada** – interrompido ou pausado.

Contador de Atualização

Tabela 80. Contador de Atualizações

Contador	Definição
avBasesAge	“Idade” dos bancos de dados (tempo decorrido em centésimos de segundos desde a data de criação da última instalação dos bancos de dados atualizados).

Contadores de Proteção em Tempo Real

Tabela 81. Contadores de Proteção em Tempo Real

Contador	Definição
totalObjectsProcessed	Número total de objetos verificados desde a execução pela última vez da tarefa Proteção de Arquivos em Tempo Real
totalInfectedObjectsFound	Número total de objetos infectados e de outros detectados desde a última execução da tarefa de Proteção de arquivos em tempo real
totalSuspiciousObjectsFound	Número total de objetos possivelmente infectados detectados desde a última execução da tarefa de Proteção de arquivos em tempo real
totalVirusesFound	Número total de objetos verificados desde a última execução da tarefa de Proteção de arquivos em tempo real
totalObjectsQuarantined	Número total de objetos infectados, possivelmente infectados e outros objetos que foram colocados na Quarentena pelo Kaspersky Embedded Systems Security 2.2; calculado a partir do momento da última inicialização da tarefa de Proteção de Arquivos em Tempo Real
totalObjectsNotQuarantined	Número total de objetos infectados ou possivelmente infectados que o Kaspersky Embedded Systems Security 2.2 tentou colocar na Quarentena mas não conseguiu; calculado a partir da hora em que foi iniciada pela última vez a tarefa Proteção de Arquivos em Tempo Real

Contador	Definição
totalObjectsDisinfected	Número total de objetos infectados desinfectados pelo Kaspersky Embedded Systems Security 2.2; calculado a partir do momento em que a tarefa de Proteção de Arquivos em Tempo Real foi executada pela última vez
totalObjectsNotDisinfected	Número total de objetos infectados e de outros objetos que o Kaspersky Embedded Systems Security 2.2 tentou desinfectar, mas não conseguiu; calculado a partir do momento da última inicialização da tarefa de Proteção de Arquivos em Tempo Real
totalObjectsDeleted	Número total de objetos infectados, possivelmente infectados e outros objetos desinfectados pelo Kaspersky Embedded Systems Security 2.2; calculado a partir do momento da última inicialização da tarefa de Proteção de Arquivos em Tempo Real
totalObjectsNotDeleted	Número total de objetos infectados, possivelmente infectados e de outros objetos que o Kaspersky Embedded Systems Security 2.2 tentou desinfectar, mas não conseguiu; calculado a partir do momento da última inicialização da tarefa de Proteção de Arquivos em Tempo Real
totalObjectsBackedUp	Número total de objetos infectados e outros objetos que foram colocados no Backup pelo Kaspersky Embedded Systems Security 2.2; calculado a partir do momento da última inicialização da tarefa de Proteção de Arquivos em Tempo Real
totalObjectsNotBackedUp	Número total de objetos infectados e de outros objetos que o Kaspersky Embedded Systems Security 2.2 tentou colocar no Backup, mas não conseguiu; calculado a partir do momento da última inicialização da tarefa de Proteção de Arquivos em Tempo Real

Interceptações SNMP

As configurações de interceptações SNMP no Kaspersky Embedded Systems Security 2.2 são resumidas na tabela abaixo.

Tabela 82. Interceptações SNMP do Kaspersky Embedded Systems Security 2.2

Interceptação	Descrição	Opções
eventThreatDetected	Foi detectado um objeto.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty

Interceptação	Descrição	Opções
eventBackupStorageSizeExceeds	Tamanho máximo do backup excedido. O tamanho total de dados no Backup excedeu o valor especificado por **Tamanho máximo do backup (MB)**. O Kaspersky Embedded Systems Security 2.2 continua a fazer backup de objetos infectados.	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	Limite de espaço disponível no backup atingido. O volume disponível no Backup atribuído pelo **Valor limite de espaço disponível (MB)** é igual ou inferior ao valor especificado. O Kaspersky Embedded Systems Security 2.2 continua a fazer backup de objetos infectados.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	Tamanho máximo da Quarentena excedido. O tamanho total dos dados da Quarentena excedeu o valor especificado por **Tamanho máximo da Quarentena (MB)**. O Kaspersky Embedded Systems Security 2.2 continua a colocar na Quarentena os objetos possivelmente infectados.	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	Limite de espaço disponível na Quarentena atingido. O volume disponível na Quarentena atribuído pelo **Valor limite de espaço disponível (MB)** é inferior ao valor especificado. O Kaspersky Embedded Systems Security 2.2 continua a colocar na Quarentena os objetos possivelmente infectados.	eventDateAndTime eventSeverity eventSource

Interceptação	Descrição	Opções
eventObjectNotQuarantined	Erro de Quarentena.	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	Erro ao salvar uma cópia de objeto no Backup.	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Erro de Quarentena.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Erro de Backup.	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	O banco de dados de antivírus está desatualizado. O número de dias desde a última execução da tarefa de atualização do banco de dados (tarefa local ou tarefa de grupo, ou tarefa para conjuntos de computadores) está sendo calculado.	eventSeverity eventDateAndTime eventSource dias

Interceptação	Descrição	Opções
eventAVBasesTotallyOutdated	O banco de dados de antivírus está obsoleto. O número de dias desde a última execução da tarefa de atualização do banco de dados (tarefa local ou tarefa de grupo, ou tarefa para conjuntos de computadores) está sendo calculado.	eventSeverity eventDateAndTime eventSource dias
eventApplicationStarted	O Kaspersky Embedded Systems Security 2.2 está sendo executado.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	O Kaspersky Embedded Systems Security 2.2 está interrompido.	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerformForALongTime	As áreas críticas não são verificadas há muito tempo. Calculado como o número de dias desde a última conclusão da *tarefa de Verificação de Áreas Críticas*.	eventSeverity eventDateAndTime eventSource dias
eventLicenseHasExpired	Licença expirou.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	A licença expira em breve. Calculado como o número de dias até a data de expiração da licença.	eventSeverity eventDateAndTime eventSource dias
eventTaskInternalError	Erro ao concluir a tarefa.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Erro ao executar uma tarefa de atualização.	eventSeverity eventDateAndTime taskName updaterErrorEventReason

A tabela abaixo descreve as configurações de interceptações e possíveis valores de parâmetros.

Tabela 83. Interceptações SNMP: valores das configurações

Configuração	Descrição e possíveis valores
eventDateAndTime	Hora do evento.
eventSeverity	Nível de importância. A configuração pode ter os seguintes valores: • critical (1) – crítico • warning (2) – aviso • info (3) – informativo
userName	Nome de usuário (por exemplo, o nome do usuário que tentou obter acesso a um arquivo infectado).
computerName	Nome do computador (por exemplo, o nome do computador a partir do qual um usuário tentou obter acesso a um arquivo infectado).
eventSource	Fonte do evento: componente funcional em que o evento foi gerado. A configuração pode ter os seguintes valores: • desconhecido (0) – componente funcional não conhecido • quarantine (1) – Quarentena • backup (2) – Backup • reporting (3) – Logs de tarefas • updates (4) – Atualização • realTimeProtection (5) – Proteção de Arquivos em Tempo Real • onDemandScanning (6) – Verificação por Demanda • product (7) – Evento relacionado com a operação do Kaspersky Embedded Systems Security 2.2 como um todo, em vez da operação de componentes individuais • systemAudit (8) – log de auditoria do sistema
eventReason	Acionador de evento: o que provocou o evento. A configuração pode ter os seguintes valores: • reasonUnknown(0) – o motivo é desconhecido • reasonInvalidSettings (1) – somente para eventos de Backup e Quarentena, é exibido se a Quarentena ou o Backup não estiver disponível (permissões de acesso insuficientes ou a pasta foi especificada incorretamente nas configurações da Quarentena -- por exemplo, um caminho de rede foi especificado). Nesse caso, o Kaspersky Embedded Systems Security 2.2 usará a pasta padrão do Backup ou da Quarentena.
objectName	Nome do objeto (por exemplo, nome do arquivo no qual o vírus foi detectado).
threatName	O nome do objeto de acordo com a classificação da Enciclopédia de Vírus. Esse nome é incluído no nome completo do objeto detectado que o Kaspersky Embedded Systems Security 2.2 retorna ao detectar um objeto. Você pode exibir o nome completo de um objeto detectado no log de tarefas (consulte a seção "Definições de configurações de log" na página 141).

Configuração	Descrição e possíveis valores
detectType	Tipo de objeto detectado. A configuração pode ter os seguintes valores: • undefined (0) – indefinido • virware – vírus clássicos e worms de rede • trojware – cavalos de Troia • malware – outros programas maliciosos • adware – software de publicidade • pornware – software de pornografia • riskware - aplicativos legítimos que podem ser usados por invasores para danificar os dados ou o computador do usuário
detectCertainty	Nível de certeza de detecção da ameaça. A configuração pode ter os seguintes valores: • Suspeita (possivelmente infectado) – o Kaspersky Embedded Systems Security 2.2 detectou uma correspondência parcial entre uma seção do código do objeto e a seção de código malicioso conhecida. • Certeza (infectado) – o Kaspersky Embedded Systems Security 2.2 detectou uma correspondência total entre uma seção no código do objeto e a seção de código malicioso conhecida.
dias	Número de dias (por exemplo, o número de dias até a data de expiração da licença).
errorCode	Código de erro.
knowledgeBaseId	Endereço de um artigo da base de dados de conhecimento (por exemplo, o endereço de um artigo que explica um erro em particular).
taskName	Nome da tarefa.
updaterErrorEventReason	Motivo para o erro de atualização. A configuração pode ter os seguintes valores: • reasonUnknown(0) – o motivo é desconhecido • reasonAccessDenied – acesso negado • reasonUrlsExhausted – a lista de fontes de atualização colapsou • reasonInvalidConfig – arquivo de configuração inválido • reasonInvalidSignature – assinatura inválida • reasonCantCreateFolder – não é possível criar pasta • reasonFileOperError – erro de arquivo • reasonDataCorrupted – objeto corrompido • reasonConnectionReset – conexão redefinida • reasonTimeOut – o tempo limite de conexão expirou • reasonProxyAuthError – erro de autenticação do servidor proxy • reasonServerAuthError – erro de autenticação do servidor • reasonHostNotFound – computador não encontrado • reasonServerBusy – servidor indisponível • reasonConnectionError – erro de conexão • reasonModuleNotFound – objeto não encontrado • reasonBlstCheckFailed(16) – erro ao verificar a lista negra de chaves. É possível que estivessem sendo publicadas atualizações ao banco de dados no momento da atualização; repita a atualização dentro de alguns minutos.

Configuração	Descrição e possíveis valores
storageObjectNotAdded EventReason	O motivo por que o objeto não foi copiado para o Backup ou colocado na Quarentena. A configuração pode ter os seguintes valores: • reasonUnknown(0) – o motivo é desconhecido • reasonStorageInternalError – erro de banco de dados; restaure o Kaspersky Embedded Systems Security 2.2. • reasonStorageReadOnly – o banco de dados é somente leitura; restaure o Kaspersky Embedded Systems Security 2.2. • reasonStorageIOError – erro de entrada-saída: a) o Kaspersky Embedded Systems Security 2.2 está corrompido, restaure o Kaspersky Embedded Systems Security 2.2; b) o disco com os arquivos do Kaspersky Embedded Systems Security 2.2 está corrompido. • reasonStorageCorrupted – o armazenamento está corrompido; restaure o Kaspersky Embedded Systems Security 2.2. • reasonStorageFull – o banco de dados está cheio; libere espaço em disco. • reasonStorageOpenError – não foi possível abrir o arquivo do banco de dados; restaure o Kaspersky Embedded Systems Security 2.2. • reasonStorageOSFeatureError – alguns recursos do sistema operacional não correspondem aos requisitos do Kaspersky Embedded Systems Security 2.2. • reasonObjectNotFound – o objeto que está sendo colocado na Quarentena não existe no disco. • reasonObjectAccessError – permissões insuficientes para usar o API de Backup: a conta sendo usada para executar a operação não tem permissões de Operador de Backup. • reasonDiskOutOfSpace – não existe espaço suficiente no disco.

Integração com WMI

O Kaspersky Embedded Systems Security 2.2 é compatível com a integração com o Windows Management Instrumentation (WMI): é possível usar sistemas cliente que usam WMI para receber dados via o padrão Web-Based Enterprise Management (WBEM) com o objetivo de reunir informações sobre o status do Kaspersky Embedded Systems Security 2.2 e seus componentes.

Quando o Kaspersky Embedded Systems Security 2.2 está instalado, ele registra o módulo proprietário no sistema, o que facilita a criação de um namespace Kaspersky Embedded Systems Security 2.2 no namespace da raiz WMI no computador local. O namespace Kaspersky Embedded Systems Security 2.2 permite trabalhar com classes e instâncias do Kaspersky Embedded Systems Security 2.2 e suas propriedades.

Os valores de algumas propriedades de instâncias dependem dos tipos de tarefa.

A *tarefa não-periódica* é uma tarefa de aplicativo não limitada em termos de tempo e que pode estar constantemente em execução ou parada. Nenhum progresso de execução existe para tais tarefas. Os resultados da execução da tarefa são registrados em log constantemente enquanto a tarefa é executada como um evento único (por exemplo, a detecção de um objeto infectado por qualquer tarefa de Proteção do Computador em Tempo Real). Este tipo de tarefa é gerenciado por meio de políticas do Kaspersky Security Center.

A *tarefa periódica* é uma tarefa de aplicativo limitada em termos de tempo e cujo progresso de execução é exibido em termos percentuais. Os resultados da tarefa são gerados quando ela é concluída e representados como um item único ou como um estado de aplicativo alterado (por exemplo, Atualização do Banco de Dados do aplicativo concluída, arquivos de configuração gerados para tarefas de geração de regra). Um número de tarefas periódicas do mesmo tipo pode estar sendo executado em um único computador simultaneamente (três tarefas de verificação por demanda com escopos da verificação diferentes). As tarefas periódicas podem ser gerenciadas por meio do Kaspersky Security Center como tarefas de grupo.

Se você usar ferramentas para gerar consultas de namespace WMI e receber dados dinâmicos de namespaces WMI na sua rede corporativa, poderá receber informações sobre o estado de aplicativo atual (consulte a tabela abaixo).

Tabela 84. Informações sobre o estado do aplicativo

Propriedade da instância	Descrição	Valores
ProductName	Nome do aplicativo instalado.	Nome completo do aplicativo sem número da versão.
ProductVersion	Versão completa do aplicativo instalada	Número da versão do aplicativo completo, inclusive o número da compilação.
InstalledPatches	Conjunto de nomes de patch exibidos, implementados para o aplicativo.	Lista de reparos críticos instalados para o aplicativo.
IsLicenseInstalled	Estado de ativação do aplicativo.	Status da chave usada para ativar o aplicativo. Valores possíveis: • Falso - Uma chave ou o código de ativação não foi estabelecido no aplicativo. • Verdadeiro - Uma chave ou o código de ativação foi adicionado ao aplicativo.
LicenseDaysLeft	Exibe quantos dias restam até a expiração da licença atual.	Número de dias restantes até a expiração da licença atual. Valores possíveis não positivos: • 0 - Licença expirou • -1 - Incapaz de obter informações sobre a chave atual ou a chave especificada não pode ser usada para ativar o aplicativo (por exemplo, foi bloqueada com base em uma lista negra de chaves).
AVBasesDatetime	Carimbo de data/hora de uma versão de banco de dados de antivírus atual.	Data e hora da criação dos bancos de dados de antivírus atualmente em uso. Se o aplicativo instalado não usar bancos de dados dw antivírus, o campo tem o valor “Não instalado”.

Propriedade da instância	Descrição	Valores
IsExploitPreventionEnabled	Estado do componente Prevenção de Exploits.	Status do componente Prevenção de Exploits. Valores possíveis: • Verdadeiro - O componente Prevenção de Exploits está ativo e fornece proteção. • Falso - O componente Prevenção de Exploits não fornece proteção. Por exemplo: desativado, não instalado, o Contrato de Licença foi violado.
ProtectionTasksRunning	Conjunto de tarefas de proteção em execução no momento.	Lista de proteção, controle e tarefas de monitoramento atualmente em execução. Este campo deve considerar todas as tarefas não periódicas em execução. Se nenhuma tarefa não periódica estiver em execução, o campo terá o valor "Não".
IsAppControlRunning	Estado da tarefa de Controle de Inicialização de Aplicativos.	Status da tarefa de Controle de Inicialização de Aplicativos. • Verdadeiro - A tarefa de Controle de Inicialização de Aplicativos está em execução. • Falso - O Controle de Inicialização de Aplicativos não está em execução ou o componente de Controle de Inicialização de Aplicativos não está instalado.
AppControlMode	Modo da tarefa de Controle de Inicialização de Aplicativos.	Descrição do status atual do componente Controle de Inicialização de Aplicativos e descreve o modo selecionado da tarefa correspondente. Valores possíveis: • Ativa - O modo **Ativa** é selecionado nas configurações de tarefa. • Somente estatísticas - O modo **Somente estatísticas** é selecionado nas configurações de tarefa. • Não instalado - O componente Controle de Inicialização de Aplicativos não está instalado
AppControlRulesNumber	O número total de regras de controle de inicialização de aplicativos.	O número de regras atualmente especificado nas configurações da tarefa de Controle de Inicialização de Aplicativos.

Propriedade da instância	Descrição	Valores
AppControlLastBlocking	O carimbo de data/hora do último bloqueio de inicialização de aplicativo pela tarefa de Controle de Inicialização de Aplicativos em qualquer modo.	Data e hora que o componente Controle de Inicialização de Aplicativos bloqueou pela última vez a inicialização de um aplicativo. Este campo inclui todos os aplicativos bloqueados, independentemente do modo da tarefa. Se nenhuma instância de inicialização de aplicativo bloqueada estiver registrada no momento em que a consulta WMI for processada, o campo recebe o valor “Não”.
PeriodicTasksRunning	O conjunto de tarefas periódicas atualmente em execução.	A lista de tarefas de Verificação por Demanda, Atualização e tarefas de tomada de inventário atualmente em execução. Este campo deve incluir todas as tarefas periódicas em execução. Se nenhuma tarefa periódica estiver sendo executada no momento, o campo recebe o valor "Não".
ConnectionState	O estado da conexão entre componente Provedor WMI e o Kaspersky Security Service (KAVFS).	Informações sobre o status da conexão entre o módulo do Provedor de WMI e o Kaspersky Security Service. Valores possíveis: • Êxito - a conexão foi estabelecida com êxito: o cliente WMI pode receber informações sobre o status de aplicativo. • Falha. Código de erro: <código> - A conexão não pode ser estabelecida devido a um erro com o código especificado.

Estes dados representam propriedades KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security, em que:

- KasperskySecurity_ProductInfo é o nome da classe do Kaspersky Embedded Systems Security 2.2
- .ProductName=Kaspersky Embedded Systems Security é o parâmetro da chave do Kaspersky Embedded Systems Security 2.2

A instância é criada no namespace ROOT\Kaspersky\Security.

Entrando em contato com o Suporte Técnico

Esta seção descreve as formas de receber suporte técnico e as condições em que ele está disponível.

Neste capítulo

Como obter suporte técnico

Se você não encontrar uma solução para seu problema na documentação do aplicativo ou em uma das fontes de informações sobre o aplicativo, é recomendável entrar em contato com o Suporte Técnico. Os especialistas do Suporte Técnico responderão a suas dúvidas sobre a instalação e o uso do aplicativo.

O suporte técnico só está disponível para os usuários que compraram uma licença comercial para o aplicativo. O suporte técnico não está disponível para os usuários com uma licença de avaliação.

Antes de entrar em contato com o Suporte Técnico, leia todas as regras do Suporte Técnico.

Você pode entrar em contato com o Suporte Técnico de uma das seguintes maneiras:

- Ligando para o Suporte Técnico.
- Enviando uma solicitação ao Suporte Técnico da Kaspersky Lab por meio do portal Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Suporte Técnico por meio do Kaspersky CompanyAccount

O Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) é um portal para empresas que usam aplicativos da Kaspersky Lab. O Kaspersky CompanyAccount destina-se a facilitar a interação entre os usuários e os especialistas do Kaspersky Lab através de solicitações online. O Kaspersky CompanyAccount permite monitorar o andamento do processamento de solicitações eletrônicas pelos especialistas da Kaspersky Lab e permite armazenar um histórico de solicitações eletrônicas.

Você pode registrar todos os funcionários de sua organização em uma única conta de usuário no Kaspersky CompanyAccount. Uma única conta permite gerenciar de forma centralizada as solicitações eletrônicas de funcionários registrados para a Kaspersky Lab e também gerenciar os privilégios desses funcionários através do Kaspersky CompanyAccount.

O Web 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 http://support.kaspersky.com/faq/companyaccount_help.

Usando arquivos de rastreamento e scripts do AVZ

Após reportar um problema aos especialistas de Suporte Técnico da Kaspersky Lab, eles poderão solicitar que você crie um relatório com informações sobre a operação do Kaspersky Embedded Systems Security 2.2 e que o envie ao Suporte Técnico da Kaspersky Lab. Além disso, os especialistas do Suporte Técnico da Kaspersky Lab podem solicitar que você crie um arquivo de rastreamento. O arquivo de rastreamento permite monitorar o processo de como os comandos do aplicativo estão sendo executados, por etapas, para determinar o momento em que ocorre o erro na operação do aplicativo.

Após analisar os dados enviados, os especialistas do Suporte Técnico da Kaspersky Lab podem criar um script AVZ e enviá-lo para você. Com scripts AVZ, é possível analisar os processos ativos quanto à existência de ameaças, verificar o computador para detectar ameaças, desinfectar ou excluir arquivos infectados e criar relatórios de verificação do sistema.

Para um suporte e resolução de problemas de aplicativo mais eficientes, os especialistas do Suporte Técnico podem solicitar que você modifique a configuração do aplicativo temporariamente com objetivos de depuração durante o diagnóstico. Para isso, pode ser necessária a realização do seguinte:

- Ativação da funcionalidade que processa e armazena informações estendidas de diagnóstico.
- Controle detalhado das configurações de componentes individuais de software, que não estão disponíveis por meio de elementos padrão da interface de usuário.
- Alteração das configurações de armazenamento e transmissão de informações de diagnóstico que foram processadas.
- Configuração da interceptação e registro de tráfego de rede em log.

AO Kaspersky Lab

A Kaspersky Lab é um fornecedor de renome mundial de sistemas de proteção de computadores contra várias ameaças digitais, incluindo ataques de vírus, malware, e-mail não solicitado (spam), ataques de rede e de hackers.

Em 2008, a Kaspersky Lab foi classificada como um dos quatro principais fornecedores de soluções de software de segurança de informações para o usuário final (IDC Worldwide Endpoint Security Revenue by Vendor). A Kaspersky Lab é o fornecedor preferencial de sistemas de proteção de computadores para usuários domésticos na Rússia (IDC Endpoint Tracker 2014).

A Kaspersky Lab foi fundada na Rússia em 1997. A partir daí, a organização se desenvolveu até se transformar em um grupo internacional de empresas com 38 escritórios em 33 países. A empresa emprega hoje mais de 3.000 especialistas qualificados.

Produtos. Os produtos da Kaspersky Lab oferecem proteção para todos os tipos de sistemas: de computadores domésticos a grandes redes corporativas.

A linha de produtos pessoais inclui aplicativos de segurança para computadores desktop, laptop e tablet, além de smartphones e outros dispositivos móveis.

A empresa oferece soluções para proteção e controle, e tecnologias para estações de trabalho e dispositivos móveis, máquinas virtuais, servidores de arquivos e servidores da web, gateways de correio e firewalls. O portfólio da empresa também inclui produtos especializados que fornecem proteção contra-ataques de DDoS, proteção para sistemas de controle industriais e contra fraude financeira. Usadas em conjunto com ferramentas de gestão centralizadas, estas soluções asseguram a proteção automatizada eficaz de empresas e organizações de qualquer porte contra ameaças de computador. Os produtos da Kaspersky Lab são certificados pelos principais laboratórios de testes, compatíveis com aplicativos de diversos fornecedores de software e otimizados para funcionar na maioria das plataformas de hardware.

Os analistas de vírus da Kaspersky Lab trabalham incansavelmente. Todos os dias, eles descobrem centenas de milhares de novas ameaças de computador, criam ferramentas para detectá-las e desinfectá-las e incluem as assinaturas destas ameaças nos bancos de dados usados pelos aplicativos da Kaspersky Lab.

Tecnologias. Várias tecnologias que agora são parte integrante de modernas ferramentas antivírus foram originalmente desenvolvidas pela Kaspersky Lab. Não é nenhuma coincidência que muitos outros desenvolvedores usem o motor do Kaspersky Antivírus nos seus produtos, incluindo: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu e ZyXEL. Muitas das tecnologias inovadoras da empresa são patenteadas.

Realizações. Ao longo dos anos, a Kaspersky Lab recebeu centenas de prêmios por seus serviços no combate às ameaças de computador. Após testes e pesquisas realizadas pelo renomado laboratório de testes austríaco AV-Comparatives em 2014, a Kaspersky Lab ficou entre os dois principais fornecedores pelo número de certificados Advance+ obtidos e, ao final, recebeu o certificado de Melhor Classificação. Mas a principal realização da Kaspersky Lab é a fidelidade de seus usuários em todo o mundo. Os produtos e as tecnologias da empresa protegem mais de 400 milhões de usuários, e seus clientes corporativos somam mais de 270.000.

Site da Kaspersky Lab:	https://www.kaspersky.com.br/
Enciclopédia de Vírus	https://securelist.com
Laboratório de Vírus:	https://virusdesk.kaspersky.com (para analisar arquivos e sites suspeitos)
Fórum da Kaspersky Lab na Web:	https://forum.kaspersky.com

Informações sobre código de terceiros

As informações sobre códigos de terceiros estão contidas no arquivo legal_notices.txt, na pasta de instalação do aplicativo.

Notificações de marcas registradas

As marcas registradas e marcas de serviço são propriedade de seus respectivos proprietários.

Intel e Pentium são marcas registradas da Intel Corporation nos Estados Unidos e/ou em outros países.

Microsoft Active Directory, Excel, Internet Explorer, Outlook, Windows, Windows Server e Windows Vista são marcas registradas da Microsoft Corporation nos Estados Unidos e em outros países.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e em outros países.

Glossário

A

Analisador heurístico

Tecnologia de detecção de ameaças cujas informações ainda não foram adicionadas aos bancos de dados da Kaspersky Lab. O analisador heurístico detecta objetos cujo comportamento no sistema pode representar uma ameaça de segurança. Os objetos detectados pelo analisador heurístico são considerados como possivelmente infectados. Por exemplo, um objeto pode ser considerado possivelmente infectado se contiver sequências de comandos típicos de objetos maliciosos (abrir arquivo, gravar no arquivo).

Arquivo comprimido ou compactado

Um ou vários arquivos empacotados em um arquivo único por meio da compactação. Um aplicativo dedicado, chamado arquivador, é necessário para empacotar e desempacotar os dados.

Arquivo infectável

Um arquivo que, devido à sua estrutura ou ao seu formato, pode ser usado por criminosos como um "contêiner" para armazenar e distribuir código malicioso. Geralmente, estes são arquivos executáveis, com extensões como .com, .exe, e .dll. O risco da penetração de código malicioso em tais arquivos é bastante alto.

Atualização

Procedimento para substituir/adicionar novos arquivos (bancos de dados ou módulos do aplicativo) recuperados de servidores de atualização da Kaspersky Lab.

B

Backup

Armazenamento especial de cópias de backup de arquivos criadas antes da tentativa de desinfecção ou exclusão.

Bancos de dados de Antivírus

Bancos de dados que contêm informações sobre ameaças à segurança do computador conhecidas pela Kaspersky Lab na data de publicação dos bancos de dados de antivírus. As entradas dos bancos de dados de antivírus permitem detectar código malicioso em objetos verificados. Os bancos de dados de Antivírus são criados pelos peritos da Kaspersky Lab e atualizados de hora em hora.

C

Chave ativa

Uma chave usada atualmente pelo aplicativo.

Configurações de tarefa

Configurações do aplicativo específicas para cada tipo de tarefa.

D

Desinfecção

Método de processamento de objetos infectados que resulta na recuperação completa ou parcial dos dados. Nem todos os objetos infectados podem ser desinfectados.

F

Falso positivo

Uma situação em que o aplicativo da Kaspersky Lab considera um objeto não infectado como infectado devido à semelhança de seu código com o código de um vírus.

G

Gravidade do evento

Propriedade de um evento encontrado durante a operação de um aplicativo da Kaspersky Lab. Há quatro níveis de gravidade:

- Evento crítico;
- Erro;
- Aviso;
- Informação.

Os eventos do mesmo tipo podem ter níveis de gravidade diferentes dependendo da situação na qual o evento ocorreu.

K

Kaspersky Security Network (KSN)

Uma infraestrutura de serviços na nuvem que fornece acesso ao banco de dados da Kaspersky Lab com informações constantemente atualizadas sobre a reputação de arquivos, recursos da web e software. A Kaspersky Security Network garante respostas mais rápidas por aplicativos da Kaspersky Lab a ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos.

M

Máscara de arquivos

Representação de um nome de arquivo usando curingas. Os curingas padrão usados em máscaras de arquivos são * e ?, em que * representa qualquer número de caracteres e ? representa qualquer caractere.

N

Nível de segurança

O nível de segurança é definido como um conjunto predefinido de configurações de componentes do aplicativo.

O

Objetos de inicialização

Grupo de aplicativos necessários para que o sistema operacional e o software instalados no computador iniciem e funcionem corretamente. Esses objetos são executados sempre que o sistema operacional é iniciado. Há vírus capazes de infectar tais objetos especificamente, podendo levar, por exemplo, ao bloqueio da inicialização do sistema operacional.

Objeto infectado

Um objeto com uma porção de código que corresponde completamente a uma porção de código de um malware conhecido. A Kaspersky Lab não recomenda usar estes objetos.

Objeto OLE

Um objeto anexado ou incorporado a outro arquivo usando a tecnologia OLE (Object Linking and Embedding). Um exemplo de objeto OLE é uma planilha do Microsoft Excel® incorporada a um documento do Microsoft Word.

P

Período da licença

Período de tempo durante o qual você tem acesso aos recursos do aplicativo e direitos de uso dos serviços adicionais. Os serviços que você pode usar dependem do tipo da licença.

Política

Uma política determina as configurações de um aplicativo e gerencia o acesso à configuração de um aplicativo instalado em computadores dentro de um grupo de administração. Uma política individual deve ser criada para cada aplicativo. 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 dentro de um grupo de administração.

Proteção em Tempo Real

Modo de operação do aplicativo no qual os objetos são verificados quanto à presença de código malicioso em tempo real.

O aplicativo intercepta todas as tentativas de abrir qualquer objeto (ler, escrever ou executar) e verifica o objeto para ameaças. Os objetos não infectados são transmitidos ao usuário; os objetos que contêm ameaças ou objetos possivelmente infectados são processados segundo as configurações da tarefa (desinfectado, excluído ou colocado em Quarentena).

Q

Quarentena

A pasta para onde o aplicativo da Kaspersky Lab move objetos possivelmente infectados que foram detectados. Os objetos são armazenados na Quarentena em formato criptografado para evitar qualquer impacto negativo no computador.

S

Servidor de Administração

Um componente do Kaspersky Security Center que armazena de modo centralizado informações sobre todos os aplicativos da Kaspersky Lab instalados na rede corporativa. Ele também pode ser usado para gerenciar tais aplicativos.

SIEM

Uma tecnologia que analisa eventos de segurança originados em vários dispositivos de rede e aplicativos.

Status da proteção

O status de proteção atual que reflete o nível da segurança do computador.

T

Tarefa

As funções executadas pelo aplicativo da Kaspersky Lab são implementadas como tarefas, por exemplo: Proteção de arquivos em tempo real, Verificação completa do computador e Atualização do banco de dados.

Tarefa local

Uma tarefa definida e executada em um computador cliente único.

V

Vulnerabilidade

Uma falha no sistema operacional ou em um aplicativo que pode ser explorada por desenvolvedores de malware para penetrar no sistema operacional ou em aplicativos e corromper sua integridade. A presença de um grande número de vulnerabilidades em um sistema operacional torna-o pouco confiável, já que os vírus que penetrarem nele poderão causar problemas no próprio sistema operacional e nos aplicativos instalados.

Índice

D

N