kaspersky

Kaspersky Embedded Systems Security 3.3 for Windows

Índice

Sobre o Kaspersky Embedded Systems Security for Windows

O Kaspersky Embedded Systems Security for Windows protege computadores e outros sistemas incorporados do Microsoft® Windows® (doravante referidos como dispositivos protegidos) contra vírus e outras ameaças de computador. Os usuários do Kaspersky Embedded Systems Security for Windows são administradores da rede corporativa e especialistas responsáveis pela proteção antivírus da rede corporativa.

O aplicativo não é voltado para o uso em processos tecnológicos que envolvam sistemas de controle automatizados. Para proteger os dispositivos nesses sistemas, é recomendável usar o aplicativo Kaspersky Industrial CyberSecurity for Nodes.

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

- Caixas eletrônicos.
- PDV (Pontos De Venda)

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

- Por meio do Console do Aplicativo instalado no mesmo dispositivo protegido em que o Kaspersky Embedded Systems Security for Windows está instalado ou em um dispositivo 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 dispositivos protegidos executando o Kaspersky Embedded Systems Security for Windows.

É possível examinar os Contadores de desempenho do Kaspersky Embedded Systems Security for Windows para o aplicativo "Monitor do Sistema", além de Medidores e interceptações SNMP.

Componentes e funções do Kaspersky Embedded Systems Security for Windows

O aplicativo inclui os seguintes componentes:

- **Proteção de Arquivos em Tempo Real**. O Kaspersky Embedded Systems Security for Windows verifica objetos quando eles são acessados. O Kaspersky Embedded Systems Security for Windows verifica os seguintes objetos:
  - Arquivos.
  - Fluxos alternativos do sistema de arquivos (Fluxos NTFS)
  - Registros mestres de inicialização e setores de inicialização nos discos rígidos locais e unidades removíveis
- **Verificação por demanda**. O Kaspersky Embedded Systems Security for Windows executa uma única verificação da área especificada quanto à existência de vírus e outras ameaças à segurança do computador. O aplicativo verifica os arquivos, a RAM e os objetos de execução automática em um dispositivo protegido.
- **Controle de Inicialização de Aplicativos**. O componente monitora as tentativas do usuário de iniciar aplicativos e regula a inicialização de aplicativos no dispositivo protegido.

- **Controle de Dispositivos**. O componente controla o registro e o uso de dispositivos externos para proteger o dispositivo contra ameaças à segurança que possam surgir enquanto os arquivos são trocados com pendrives conectados por USB ou outros tipos de dispositivos externos.

- **Gerenciamento de firewall**. O componente oferece a capacidade de gerenciar o Firewall do Windows: definir as configurações e regras do firewall do sistema operacional e bloquear qualquer possibilidade de configuração externa do firewall.

- **Monitor de Integridade de Arquivos**. O Kaspersky Embedded Systems Security for Windows detecta mudanças nos arquivos dentro dos escopos de monitoramento especificados nas configurações da tarefa. Essas mudanças podem indicar uma violação de segurança no dispositivo 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 a seguir são implementadas no aplicativo:

- **Atualização do Banco de Dados** e **Atualização dos Módulos de Software**. O Kaspersky Embedded Systems Security for Windows baixa atualizações de bancos de dados e módulos do aplicativo a partir dos servidores de atualização FTP ou HTTP da Kaspersky, do Servidor de Administração do Kaspersky Security Center ou de outras fontes de atualização.

- **Quarentena**. O Kaspersky Embedded Systems Security for Windows coloca em Quarentena objetos possivelmente infectados, movendo-os da sua localização original para a pasta de *Quarentena*. Por motivos de segurança, os objetos na pasta Quarentena são armazenados em formato criptografado.

- **Backup**. O Kaspersky Embedded Systems Security for Windows armazena cópias criptografadas de objetos classificados como *Infectados* no *Backup* antes de desinfectá-los ou excluí-los.

- **Notificações do administrador e dos usuários**. É possível configurar o aplicativo para notificar o administrador e usuários que acessem o dispositivo protegido quanto aos eventos relativos à operação do Kaspersky Embedded Systems Security e o status da proteção do antivírus do dispositivo.

- **Configurações de importação e exportação**. Você pode exportar as configurações do Kaspersky Embedded Systems Security for Windows para um arquivo de configuração XML e importar configurações para o Kaspersky Embedded Systems Security for Windows a partir do arquivo de configuração. É possível salvar todas as configurações do aplicativo ou apenas aquelas de componentes individuais como um arquivo de configuração.

- **Aplicando modelos**. É possível definir manualmente as configurações de segurança de um nó na árvore ou em uma lista dos recursos de arquivos do dispositivo protegido e salvar os valores das configurações como um modelo. O modelo pode então ser utilizado para especificar as configurações de segurança de outros nodes nas tarefas de proteção e de verificação do Kaspersky Embedded Systems Security for Windows.

- **Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security for Windows**. É possível configurar os direitos para gerenciar o Kaspersky Embedded Systems Security for Windows e os serviços do Windows registrados pelo aplicativo para usuários e grupos de usuários.

- **Gravação de eventos no Log de eventos do Windows**. O Kaspersky Embedded Systems Security for Windows 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 for Windows e informações necessárias para o diagnóstico de erros no Kaspersky Embedded Systems Security for Windows.

- **Zona Confiável**. É possível gerar uma lista de exclusões do escopo da verificação ou da proteção que será aplicada pelo Kaspersky Embedded Systems Security for Windows às tarefas de Proteção do Computador em Tempo Real e Por Demanda.

- **Prevenção de Exploits**. É possível proteger a memória do processo contra exploits usando um Agente de Proteção injetado no processo.

O que há de novo

A nova versão do Kaspersky Embedded Systems Security for Windows apresenta os seguintes novos recursos e aprimoramentos:

- Na tarefa de Proteção Contra Ameaças à Rede, a proteção contra ataques de spoofing de endereço MAC foi adicionada.
- Na tarefa de Gerenciamento do Firewall, é possível selecionar o modo de interação com o Firewall do Windows – **Monitorar o status do Firewall do Windows** ou **Controlar o Firewall do Windows**.
- Para a tarefa do Monitor de Integridade de Arquivos, a capacidade de exportar regras para um arquivo externo e importar regras de um arquivo externo foi adicionada.
- Para a tarefa do Monitor de Acesso ao Registro, a capacidade de exportar regras para um arquivo externo e importar regras de um arquivo externo foi adicionada.
- As regras de processo confiável agora podem ser aplicadas à tarefa de Controle de Inicialização de Aplicativos. As tarefas do Monitor de Acesso ao Registro e do Monitor de Integridade de Arquivos sempre aplicam as configurações da zona confiável. As configurações para a aplicabilidade das regras de processo confiável às tarefas do Monitor de Integridade de Arquivos e Monitor de Acesso ao Registro não estão mais disponíveis. As configurações de aplicabilidade das regras de processo confiável agora estão localizadas nas configurações da zona confiável.
- Na tarefa de Controle de Inicialização de Aplicativos, uma opção para filtrar por nome de grupo de dispositivos foi adicionada ao criar as regras de acordo com os eventos no log do Kaspersky Security Center.
- No Kaspersky Security Center Web Console, nas configurações de regras da tarefa de Controle de Inicialização de Aplicativos, agora é possível adicionar as regras de permissão de acordo com os eventos no log do Kaspersky Security Center.
- No plug-in para gerenciamento do aplicativo pelo Kaspersky Security Center, a lista de fontes de informações do usuário foi estendida nas configurações de regra e tarefa para as tarefas de Controle de Inicialização de Aplicativos, Controle de Dispositivo, Monitor de Integridade de Arquivos e Monitor de Acesso ao Registro. Agora, o administrador pode não só especificar os usuários das listas do Active Directory, mas também selecionar os usuários das listas de contas do Kaspersky Security Center ou especificar o nome de usuário ou o grupo de usuários manualmente.
- Os eventos de detecção de ameaças no modo “Somente notificações sobre ataques detectados” para a tarefa Proteção Contra Ameaças à Rede são publicados agora com o nível de importância “Aviso” em vez de “Crítico”.
- O número de eventos das tarefas Monitor de Acesso ao Registro e Monitor de Integridade de Arquivos foi otimizado. Eventos duplicados não são enviados ao Kaspersky Security Center, mas somente aos logs de tarefa.
- Suporte para novos sistemas operacionais: Windows 11 23H2, Windows 11 23H2 IoT.
- O aplicativo notifica o usuário quando o período de suporte para a versão instalada do aplicativo expira.
- O plug-in para gerenciar o aplicativo pelo Kaspersky Security Center não é mais compatível com a criação de uma política pela exportação de propriedades da política de um arquivo KLP. No entanto, isso ainda pode ser feito usando o Assistente de Nova Política no console de administração do Kaspersky Security Center.
- Os problemas das versões anteriores foram resolvidos: esta versão do aplicativo inclui correções das versões anteriores.

Fontes de informação sobre o Kaspersky Embedded Systems Security for Windows

Esta seção lista 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.

Fontes para a recuperação independente de informações

Você pode usar as fontes a seguir para encontrar informação sobre o Kaspersky Embedded Systems Security for Windows:

- Acesse a página do Kaspersky Embedded Systems Security for Windows no site da Kaspersky.
- Página do Kaspersky Embedded Systems Security for Windows no site do Suporte Técnico (Base de dados de conhecimento).
- Manuais.

Caso não tenha encontrado uma solução para o problema, entre em contato com o Suporte Técnico da Kaspersky.

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

Acesse a página do Kaspersky Embedded Systems Security for Windows no site da Kaspersky

Na página do Kaspersky Embedded Systems Security for Windows, é possível visualizar as informações gerais sobre o aplicativo, as funções e os recursos.

A página do Kaspersky Embedded Systems Security for Windows contém um link para a loja on-line. Lá, você pode comprar o aplicativo ou renovar sua licença.

Página do Kaspersky Embedded Systems Security for Windows na base de dados de conhecimento

A base de dados de conhecimento é uma seção do site de Suporte Técnico.

Na página do Kaspersky Embedded Systems Security for Windows, na base de dados de conhecimento, é possível encontrar artigos com informações úteis, recomendações e respostas a perguntas frequentes sobre a compra, instalação e uso do aplicativo.

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

Documentação do Kaspersky Embedded Systems Security for Windows

O guia do administrador do Kaspersky Embedded Systems Security for Windows contém informações sobre a instalação, desinstalação, configuração e uso do aplicativo.

Discussão sobre os aplicativos da Kaspersky no fórum

É possível discutir questões relativas aos aplicativos da Kaspersky com outros usuários e especialistas da Kaspersky no nosso Fórum.

Em nosso Fórum, é possível visualizar os tópicos existentes, deixar comentários e criar novos tópicos de discussão.

Kaspersky Embedded Systems Security for Windows

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

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 for Windows.
- Iniciar o Assistente de instalação do Console do Kaspersky Embedded Systems Security for Windows.
- Iniciar o assistente de instalação que instalará o Plug-in de Administração do Kaspersky Embedded Systems Security for Windows para gerenciar o aplicativo pelo Kaspersky Security Center.
- Acesse a página do Kaspersky Embedded Systems Security for Windows no site da Kaspersky.
- Visitar o site de Suporte Técnico.
- Leia as informações sobre a versão atual do Kaspersky Embedded Systems Security for Windows.

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

Arquivos do kit de distribuição do Kaspersky Embedded Systems Security for Windows

Arquivo	Finalidade
autorun.inf	Arquivo de execução automática para o Assistente de instalação do Kaspersky Embedded Systems Security for Windows ao instalar o aplicativo a partir de uma unidade removível.
release_notes.txt	O arquivo contém informações da versão.
migration.txt	O arquivo descreve a migração de versões anteriores do aplicativo.
setupui.exe	Arquivo de inicialização do programa de boas-vindas (inicia setup.hta).
ess.kud	Arquivo no formato Kaspersky Unicode Definition com uma descrição do pacote de instalação para a instalação remota do aplicativo através do Kaspersky Security Center.
\console\esstools.msi	Pacote do Windows Installer. Instala o Console do Aplicativo no dispositivo gerenciado.
\console\setup.exe	Arquivo de inicialização para um assistente que instala um conjunto de componentes das Ferramentas de Administração (incluindo o Kaspersky Embedded Systems Security for Windows). O arquivo do pacote de instalação esstools.msi é iniciado com as configurações de instalação especificadas no assistente.
\exec\bases.cab	Arquivo comprimido dos bancos de dados de antivírus atuais do antivírus no momento da liberação do aplicativo.
\exec\config.ini	Arquivo de configuração com parâmetros de instalação para a criação do pacote de instalação do Kaspersky Embedded Systems Security

	for Windows no Kaspersky Security Center.
\exec\ess.kud	Arquivo no formato Kaspersky Unicode Definition com uma descrição do pacote de instalação para a instalação remota do Kaspersky Embedded Systems Security for Windows através do Kaspersky Security Center.
\exec\ess_x64.msi	Pacote do Windows Installer. Instala o Kaspersky Embedded Systems Security for Windows no dispositivo gerenciado que executa um sistema operacional Microsoft Windows de 64 bits.
\exec\ess_x86.msi	Pacote do Windows Installer. Instala o Kaspersky Embedded Systems Security for Windows no dispositivo gerenciado que executa um sistema operacional Microsoft Windows de 32 bits.
\exec\klcfginst.exe	Instalador para Plug-in de administração para gerenciar o aplicativo através do Kaspersky Security Center.
\exec\license.txt	Arquivo com o texto do Contrato de Licença do Usuário Final e Política de Privacidade.
\exec\setup.exe	O arquivo para instalação do Kaspersky Embedded Systems Security for Windows no dispositivo protegido, por meio do assistente; ele inicializa o arquivo do pacote de instalação ess.msi com as configurações de instalação especificadas no assistente.
\product_long_term\config.ini	Arquivo de configuração com parâmetros de instalação para a criação do pacote de instalação do Kaspersky Embedded Systems Security for Windows no Kaspersky Security Center.
\product_long_term\ess_light.kud	Arquivo no formato Kaspersky Unicode Definition com uma descrição do pacote de instalação para a instalação remota do Kaspersky Embedded Systems Security for Windows através do Kaspersky Security Center.
\product_long_term\ess_x86.msi	Pacote do Windows Installer. Instala a configuração **Proteger o computador com a tecnologia de Negação padrão** do Kaspersky Embedded Systems Security for Windows no dispositivo protegido que executa um sistema operacional de 32 bits.

	Os componentes que ativam atualizações não estão incluídos na configuração Proteger o computador com tecnologia de Negação padrão. Se a configuração Proteger o computador com tecnologia de Negação padrão estiver selecionada, os seguintes componentes serão incluídos por padrão: • Core • Prevenção de Exploits • Controle de Inicialização de Aplicativos • Ícone da bandeja do sistema Quando a configuração "Proteger o computador com a tecnologia de Negação padrão" do aplicativo é instalada sobre uma versão do aplicativo que usa análise de assinatura e bancos de dados de antivírus para proteger o computador, o conjunto de componentes do aplicativo será reduzido automaticamente pela remoção dos seguintes componentes: • Proteção de Arquivos em Tempo Real • Verificação por Demanda • os componentes que permitem atualizações Essa configuração é recomendada para proteger dispositivos com recursos limitados. Nesse caso, você pode ativar o aplicativo por um longo período, e o componente Controle de Inicialização de Aplicativos fornece proteção ao computador.
\product_long_term\ess_x64.msi	Pacote do Windows Installer. Instala a configuração **Proteger o computador com a tecnologia de Negação padrão** do Kaspersky Embedded Systems Security for Windows no dispositivo protegido que executa um sistema operacional de 64 bits.

	Os componentes que ativam atualizações não estão incluídos na configuração Proteger o computador com tecnologia de Negação padrão. Se a configuração Proteger o computador com tecnologia de Negação padrão estiver selecionada, os seguintes componentes serão incluídos por padrão: • Core • Prevenção de Exploits • Controle de Inicialização de Aplicativos • Ícone da bandeja do sistema Quando a configuração "Proteger o computador com a tecnologia de Negação padrão" do aplicativo é instalada sobre uma versão do aplicativo que usa análise de assinatura e bancos de dados de antivírus para proteger o computador, o conjunto de componentes do aplicativo será reduzido automaticamente pela remoção dos seguintes componentes: • Proteção de Arquivos em Tempo Real • Verificação por Demanda • os componentes que permitem atualizações Essa configuração é recomendada para proteger dispositivos com recursos limitados. Nesse caso, você pode ativar o aplicativo por um longo período, e o componente Controle de Inicialização de Aplicativos fornece proteção ao computador.
\product_long_term\klcfginst.exe	Instalador para Plug-in de administração para gerenciar o aplicativo através do Kaspersky Security Center.
\product_long_term\license.txt	Arquivo com o texto do Contrato de Licença do Usuário Final e Política de Privacidade.
\product_long_term\setup.exe	Arquivo para instalação do Kaspersky Embedded Systems Security for Windows no dispositivo protegido usando o assistente de instalação; ele inicializa o arquivo do pacote de instalação ess.msi com as configurações de instalação especificadas no assistente.
\setup\images	Pasta com os arquivos de inicialização da tela de boas-vindas do aplicativo.
\setup\setup.hta	Arquivo de inicialização da tela de boas-vindas do aplicativo.
\setup\SETUP_STRINGS.JS	Arquivo com os recursos de texto do aplicativo.

Requisitos de hardware e software

Antes de instalar o Kaspersky Embedded Systems Security for Windows, você deve desinstalar outros aplicativos antivírus do dispositivo.

Requisitos de software para o dispositivo protegido

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

O Windows Installer 3.1 é necessário para a instalação e operação adequadas do aplicativo em um dispositivo protegido que executa o Microsoft Windows XP.

Para instalar e usar o Kaspersky Embedded Systems Security for Windows nos dispositivos protegidos com sistemas operacionais incorporados, é necessário ter o componente Gerenciador de Filtro.

Para a operação correta do Kaspersky Embedded Systems Security for Windows, o suporte a SHA-2 é necessário no Windows. Para obter informações detalhadas, consulte: https://support.kaspersky.com/15728.

É possível instalar o Kaspersky Embedded Systems Security for Windows em um dispositivo que executa um dos seguintes sistemas operacionais Microsoft Windows 32 ou 64 bits:

- Estações de trabalho:
  - Windows XP Pro SP2 32 bits/64 bits
  - Windows XP Pro SP3 32 bits
  - Windows 7 Professional/Enterprise/Ultimate SP1 32 bits/64 bits
  - Windows 8 Pro/Enterprise 32 bits/64 bits
  - Windows 8.1 Pro/Enterprise 32 bits/64 bits
  - Windows 10 versão 1507 Home/Pro/Education/Enterprise 32 bits/64 bits
  - Windows 10 LTSC 2015 versão 1507 32 bits/64 bits
  - Windows 10 RS1 versão 1607 Home/Pro/Education/Enterprise 32 bits/64 bits
  - Windows 10 LTSC 2016 versão 1607 32 bits/64 bits
  - Windows 10 RS2 versão 1703 Home/Pro/Education/Enterprise de 32 bits/64 bits
  - Windows 10 RS3 versão 1709 Home/Pro/Education/Enterprise 32 bits/64 bits

- Windows 10 RS4 versão 1803 Home/Pro/Education/Enterprise 32 bits/64 bits
- Windows 10 RS5 versão 1809 Home/Pro/Education/Enterprise 32 bits/64 bits
- Windows 10 LTSC 2019 versão 1809 32 bits, 64 bits
- Windows 10 19H2 versão 1909 Home/Pro/Education/Enterprise 32 bits/64 bits
- Windows 10 21H2 versão 21H2 Home/Pro/Education/Enterprise 32 bits/64 bits
- Windows 10 LTSC 2021 versão 21H2 de 32 bits/64 bits
- Windows 10 22H2 versão 22H2 Home/Pro/Education/Enterprise 32 bits/64 bits
- Windows 11 21H2 versão 21H2 Home/Pro/Education/Enterprise 64 bits
- Windows 11 22H2 versão 2H2 Home/Pro/Education/Enterprise 64 bits
- Windows 11 23H2 versão 23H2 Home / Pro / Education / Enterprise 64 bits

- Sistemas integrados:
  - Windows XP Embedded SP2 (WEPOS) 32 bits/64 bits
  - Windows XP Embedded SP3 (POS Ready 2009) 32 bits
  - Windows 7 Embedded SP1 (POSReady 7) 32 bits/64 bits
  - Windows 8.0 Embedded Industry Pro 32 bits/64 bits
  - Windows 8.1 Embedded Industry Pro 32 bits/64 bits
  - Windows 10 versão 1507 IoT Enterprise 32 bits/64 bits
  - Windows 10 versão 1607 IoT Enterprise 32 bits/64 bits
  - Windows 10 versão 1703 IoT Enterprise 32 bits/64 bits
  - Windows 10 versão 1709 IoT Enterprise 32 bits/64 bits
  - Windows 10 versão 1803 IoT Enterprise 32 bits/64 bits
  - Windows 10 versão 1809 IoT Enterprise 32 bits/64 bits
  - Windows 10 versão 1909 IoT Enterprise 32 bits/64 bits
  - Windows 10 versão 21H2 IoT Enterprise 32 bits/64 bits
  - Windows 10 versão 22H2 IoT Enterprise 32 bits/64 bits
  - Windows 11 versão 21H2 IoT Enterprise 64 bits
  - Windows 11 versão 22H2 IoT Enterprise 64 bits
  - Windows 11 versão 23H2 IoT Enterprise 64 bits

Requisitos de hardware para o dispositivo protegido

Requisitos de hardware para o dispositivo protegido

Tipo de SO	Nome do SO	Requisitos mínimos	Requisitos recomendados

Estações de trabalho	Windows XP x86/x64	• Processador: processador de core único de 1,4 GHz Pentium III (x32), Pentium IV (x64).
		• RAM:
		  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 256 MB.
		  • Para instalar todos os componentes do aplicativo – 512 MB
		• Espaço livre em disco:
		  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 50 MB.
		  • Para instalar todos os componentes do aplicativo – 2 GB
			• Processador: quad-core de 2,4 GHz
			• RAM: 2 GB
			• Espaço livre em disco:
			  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 2 GB.
			  • Para instalar todos os componentes do aplicativo – 4 GB

	Windows 7/8/10 x86	• Processador: processador de core único de 1,4 GHz Pentium III (x32), Pentium IV (x64).
		• RAM:
		  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 256 MB.
		  • Para instalar todos os componentes do aplicativo – 1 GB
		• Espaço livre em disco:
		  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 50 MB.
		  • Para instalar todos os componentes do aplicativo – 2 GB
			• Processador: quad-core de 2,4 GHz
			• RAM: 2 GB
			• Espaço livre em disco:
			  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 2 GB.
			  • Para instalar todos os componentes do aplicativo – 4 GB

	Windows 7/8/10/11 x64	• Processador: processador de núcleo único de 1,4 GHz Pentium IV (x64).
		• RAM:
		  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 1 GB.
		  • Para instalar todos os componentes do aplicativo – 2 GB
		• Espaço livre em disco:
		  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 50 MB.
		  • Para instalar todos os componentes do aplicativo – 2 GB
			• Processador: quad-core de 2,4 GHz
			• RAM:
			  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 2 GB.
			  • Para instalar todos os componentes do aplicativo – 4 GB
			• Espaço livre em disco:
			  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 2 GB.
			  • Para instalar todos os componentes do aplicativo – 4 GB

Sistemas integrados	Windows XP Embedded
	
	Windows Embedded POSReady 2009
		• Processador: processador de core único de 1,4 GHz Pentium III (x32), Pentium IV (x64).
		• RAM:
		  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 256 MB.
		  • Para instalar todos os componentes do aplicativo – 512 MB
		• Espaço livre em disco:
		  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 50 MB.
		  • Para instalar todos os componentes do aplicativo – 2 GB
			• Processador: quad-core de 2,4 GHz
			• RAM: 2 GB
			• Espaço livre em disco:
			  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 2 GB.
			  • Para instalar todos os componentes do aplicativo – 4 GB

	Windows 7/8 Embedded Windows 10 / 11 IoT	• Processador: processador de núcleo único de 1,4 GHz Pentium IV (x64). • RAM: 1 GB.	• Processador: quad-core de 2,4 GHz • RAM: 2 GB • Espaço livre em disco:

		• Espaço livre em disco:
		  • Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 50 MB.
		  • Para instalar todos os componentes do aplicativo – 2 GB
			• Para instalar apenas o componente de Controle de Inicialização de Aplicativos – 2 GB.
			• Para instalar todos os componentes do aplicativo – 4 GB

Limitação de funcionalidade em versões desatualizadas do Windows

- Ao criar um pacote de instalação no Kaspersky Security Center versão 12 e posterior, para instalar o Kaspersky Endpoint Agent em dispositivos que executam o Windows XP ou o Windows Server 2003, use o arquivo executável setup.exe do pacote de instalação criado no Kaspersky Security Center versão 10.5.
- Para gerenciar o Kaspersky Endpoint Agent usando o Kaspersky Security Center:
  - em um computador executando o Windows XP SP2 Professional (32 bits/64 bits), Windows Server 2003 ou Windows Server 2003 R2, você deve usar o Agente de Rede do Kaspersky Security Center (klnagent) versão 10.5.1781.
  - em um computador executando o Windows XP SP3 Professional (32 bits) e o Windows XP Embedded SP3 (32 bits), você deve usar o Agente de Rede do Kaspersky Security Center (klnagent) versão 14.0.0.20023.

Requisitos e limitações funcionais

Esta seção descreve os requisitos funcionais adicionais e as limitações existentes dos componentes do Kaspersky Embedded Systems Security for Windows.

Instalação e desinstalação

A seguir está a lista de limitações de instalação e desinstalação:

- Para a operação correta do Kaspersky Embedded Systems Security for Windows, o suporte a SHA-2 é necessário no Windows.
- Ao instalar o aplicativo, um aviso pode aparecer na tela se o caminho especificado para a pasta de instalação do Kaspersky Embedded Systems Security for Windows contiver mais de 150 caracteres. O aviso não afeta o processo de instalação: é possível instalar e executar o Kaspersky Embedded Systems Security for Windows.
- Se você deseja instalar o componente de suporte ao protocolo SNMP, certifique-se de reiniciar o serviço SNMP se ele estiver em execução.
- Se desejar instalar e executar o Kaspersky Embedded Systems Security for Windows em um dispositivo que executa um sistema operacional incorporado, certifique-se de instalar o componente de Gerenciador de filtros.
- Não é possível instalar as ferramentas de administração do Kaspersky Embedded Systems Security for Windows por meio das políticas de grupo do Microsoft Active Directory®.

- Se o node de Proteção antivírus for excluído da lista de componentes do aplicativo instalado, esse node desaparecerá da lista de componentes disponíveis após a conclusão da instalação. Para instalar os componentes do node de Proteção antivírus, inicie o Assistente de instalação a partir do pacote de instalação, pois contém uma lista completa de componentes.

- Caso o Console de Administração do Kaspersky Embedded Systems Security for Windows esteja instalado, o Assistente de instalação pode solicitar a reinicialização do computador. Nesse caso, a reinicialização não é obrigatória. Basta encerrar a sessão do usuário que instalou o Console de Administração e efetuar login no sistema novamente.

- Se você instalar o aplicativo nos dispositivos protegidos em execução em sistemas operacionais mais antigos, incapazes de receber atualizações periódicas, verifique se os seguintes certificados raiz estão instalados:

  - DigiCert Assured ID Root CA

  - DigiCert_High_Assurance_EV_Root_CA

  - DigiCertAssuredIDRootCA

  Caso os certificados raiz especificados não estejam instalados, o aplicativo poderá funcionar incorretamente. Recomendamos instalar os certificados o mais rápido possível.

Monitor de Integridade de Arquivos

Por padrão, o Monitor de integridade de arquivos não monitora as alterações nas pastas do sistema ou nos arquivos de manutenção do sistema de arquivos para não sobrecarregar os relatórios de tarefas com informações sobre alterações de arquivos de rotina executadas constantemente pelo sistema operacional. O usuário não pode incluir manualmente essas pastas no escopo de monitoramento.

As seguintes pastas e arquivos são excluídos do escopo de monitoramento:

- Arquivos de manutenção NTFS com id de arquivo de 0 a 33

- %SystemRoot%\Prefetch\

- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\

- %SystemRoot%\System32\LogFiles\Scm\

- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\

- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\

- %SystemRoot%\Microsoft.NET\

- %SystemRoot%\System32\config\

- %SystemRoot%\Temp\

- %SystemRoot%\ServiceProfiles\LocalService\

- %SystemRoot%\System32\winevt\Logs\

- %SystemRoot%\System32\wbem\repository\

- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\\Windows\TaskScheduler\

O aplicativo exclui as pastas de nível superior.

O componente não monitora alterações de arquivos que ignoram o sistema de arquivos ReFS/NTFS (alterações de arquivo feitas por meio de BIOS, LiveCD e mais).

Gerenciamento de Firewall

A seguir, consta uma lista de limitações para o Gerenciamento de Firewall:

- É possível especificar mais de um endereço. Caso contrário, o trabalho com IPv6 estará indisponível.
- As regras de política de Firewall predefinidas oferecem suporte a cenários básicos de interação entre dispositivos protegidos e o Servidor de Administração. Para aproveitar ao máximo as funções do Kaspersky Security Center, será necessário configurar as regras da porta manualmente. É possível encontrar informações sobre números de porta, protocolos e funções na Base de dados de conhecimento do Kaspersky Security Center.
- Após a instalação do aplicativo e configuração das regras para a tarefa, o aplicativo monitora as alterações nas regras e nos grupos de regras do Firewall do Windows quando a tarefa de Gerenciamento do Firewall é iniciada. Para atualizar o status e adicionar as regras necessárias, tenha certeza de reiniciar a tarefa de Gerenciamento de Firewall.
- Quando a tarefa de Gerenciamento de Firewall for iniciada, as regras de negação e as regras que monitoram o tráfego de saída serão automaticamente removidas das configurações de firewall do sistema operacional.
- Os caracteres "*" e "?" não podem ser usados no caminho do aplicativo e no nome da regra de firewall para o aplicativo.

Outras limitações

Limitações da **Verificação por demanda** e **Proteção de Arquivos em Tempo Real**:

- A verificação de dispositivos MTP conectados não está disponível.
- A verificação de arquivos compactados está indisponível sem a verificação do arquivo compactado SFX: caso a verificação de arquivos compactados esteja ativada nas configurações de proteção do Kaspersky Embedded

Systems Security for Windows, o aplicativo verificará automaticamente os objetos nos arquivos compactados e nos arquivos compactados SFX. A verificação de arquivos compactados SFX está disponível sem a verificação de arquivos compactados.

- Caso a caixa de seleção **Análise profunda de processos sendo inicializados (a inicialização do processo é bloqueada até que a análise termine)** e **Uso da KSN** sejam ativados simultaneamente, qualquer processo iniciado que receba o URL do endereço da Web como argumento será bloqueado, mesmo que o modo Somente Estatísticas tenha sido escolhido. Para evitar o bloqueio do processo, escolha uma das opções:

  - Desativar o **Uso da KSN**.

  - Desativar a caixa de seleção **Análise profunda de processos sendo inicializados (a inicialização do processo é bloqueada até que a análise termine)**

  Opção recomendada: desativar a caixa de seleção Análise mais aprofundada de processos sendo inicializados

Licenciamento:

- O aplicativo não pode ser ativado com uma chave por meio do Assistente de instalação caso a chave tenha sido criada usando o comando SUBST ou caso o caminho para o arquivo de chave seja um caminho de rede.

- Caso planeje usar um servidor proxy do Kaspersky Security Center para ativar o produto em um dispositivo cliente, desative a otimização de VDI nesse dispositivo ao instalar o Agente de Rede do Kaspersky Security Center.

Atualizações:

- Por padrão, o ícone do aplicativo fica oculto depois que as atualizações de módulos críticos do Kaspersky Embedded Systems Security for Windows são instaladas.

- KLRAMDISK não é compatível em dispositivos protegidos executando o sistema operacional Windows XP ou Windows Server® 2003.

Interface:

- No Console do Aplicativo, a filtragem na Quarentena, no Backup, no log de auditoria do sistema e no log de tarefas faz distinção entre maiúsculas e minúsculas.

- Ao configurar um escopo de proteção ou verificação no Console do Aplicativo, só é possível usar uma máscara e apenas no final do caminho. A seguir estão exemplos de máscaras corretas: “C:\Temp\Temp*” ou “C:\Temp\Temp???.doc” e “C:\Temp\Temp*.doc”. Essa limitação não afeta a configuração da Zona Confiável.

Segurança:

- Se o recurso de Controle de Conta de Usuário do sistema operacional for ativado, uma conta de usuário deve ser parte do grupo de Administradores KAVWSEE para abrir o Console do Aplicativo clicando duas vezes no ícone do aplicativo na área de notificação da bandeja de aplicativos. Caso contrário, será necessário fazer login como um usuário com permissão para abrir a Interface de diagnóstico compacta ou o snap-in do Console de Gerenciamento Microsoft.

- Caso o Controle de conta de usuário esteja ativado, não será possível desinstalar o aplicativo por meio da janela Programas e Recursos do Microsoft Windows.

Integração com o Kaspersky Security Center:

- Quando os pacotes de atualização são recebidos, o Servidor de Administração verifica as atualizações do banco de dados antes de enviar as atualizações para os dispositivos protegidos na rede. O Servidor de

Administração não verifica as atualizações dos módulos de software.

- Tenha certeza de que as caixas de seleção necessárias estejam marcadas nas configurações de Interação com o Servidor de Administração ao usar os componentes que transmitem dados dinâmicos ao Kaspersky Security Center usando listas de rede (Quarentena, Backup).

Prevenção de Exploits:

- A Prevenção de Exploit não está disponível se as bibliotecas apphelp.dll não forem carregadas na configuração de ambiente atual.

- O componente Prevenção de Exploit é incompatível com o utilitário EMET da Microsoft em dispositivos protegidos que executam o sistema operacional Microsoft Windows 10. O Kaspersky Embedded Systems Security for Windows bloqueará o EMET caso o componente Prevenção de Exploit esteja instalado em um dispositivo protegido com o utilitário EMET instalado.

- O componente de Prevenção de Exploit é incompatível com o mecanismo de banco de dados do SQL Server® 2012. Caso o Kaspersky Embedded Systems Security for Windows seja instalado no computador com o MS SQL Server 2012, será necessário adicionar a biblioteca sqlos.dll do servidor de banco de dados na lista de exclusões na tarefa de Prevenção de Exploit.

Instalação e remoção do aplicativo

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

Sobre a atualização do Kaspersky Embedded Systems Security for Windows

Uma atualização para o Kaspersky Embedded Systems Security for Windows versão 3.3 está disponível para o aplicativo na versão 2.1 e posterior. A atualização é executada com a instalação da nova versão do aplicativo sobre a versão instalada do aplicativo e não requer a reinicialização do computador.

Por padrão, o aplicativo cria uma nova pasta de instalação com o nome da nova versão do aplicativo de acordo com o caminho para a pasta de instalação do aplicativo existente. É possível especificar manualmente um novo caminho para a pasta de instalação do aplicativo.

Ao atualizar o Kaspersky Embedded Systems Security for Windows para a versão 3.3, a versão do aplicativo instalada anteriormente é excluída automaticamente.

Caso a versão do Kaspersky Embedded Systems Security for Windows seja anterior à 2.1, primeiro é necessário desinstalar o aplicativo instalado antes de instalar a nova versão.

Ao atualizar o Kaspersky Embedded Systems Security for Windows versão 2.1 ou posterior, protegido por senha, é necessário passar a senha ao instalador.

Ao atualizar o aplicativo, a licença atual é automaticamente aplicada ao Kaspersky Embedded Systems Security for Windows versão 3.3, e o uso dos novos componentes e tarefas do aplicativo fica totalmente disponível. O prazo da licença permanece inalterado.

Caso um aplicativo seja atualizado com uma licença expirada, a nova versão do aplicativo será executada no modo de funcionalidade limitada após a instalação (por exemplo, as atualizações do banco de dados do aplicativo não estarão disponíveis).

Migração dos valores de configurações da versão atualizada do aplicativo

As seguintes configurações permanecem inalteradas durante a atualização do aplicativo:

- configurações de aplicativo e tarefa
- logs de tarefa e logs de auditoria do sistema
- conteúdos da Quarentena e do Backup.
- contas sob as quais as tarefas são iniciadas
- permissões de acesso do usuário para o gerenciamento do aplicativo
- configurações para notificações sobre a operação de tarefas
- O serviço KAVFS continua a execução com o atributo PPL caso tenha recebido a atribuição na versão anterior do aplicativo.

As seguintes configurações são redefinidas ou alteradas para os valores padrão para a nova versão do aplicativo durante a atualização do aplicativo:

- todos os contadores, inclusive os status do banco de dados de antivírus
- dados sobre as atualizações instaladas de módulos do aplicativo e bancos de dados de antivírus
- status da tarefa
- configurações de aplicativo e tarefa configuradas pelo registro
- configurações de aplicativo e tarefa que foram alteradas durante a instalação de correções críticas.

Migração da lista de sessões de rede bloqueadas

A lista de sessões de rede bloqueadas de computadores cliente não é migrada durante uma atualização do aplicativo.

As configurações para desbloquear automaticamente o acesso aos recursos de arquivo de rede bloqueados permanecem inalteradas durante uma atualização do aplicativo.

Migração das configurações e regras do Controle de Inicialização de Aplicativos

Durante a atualização de um aplicativo, as regras do Controle de Inicialização de Aplicativos são migradas sem alterações.

Ao atualizar o aplicativo, recomendamos a interrupção da tarefa de Controle de Inicialização de Aplicativos, caso ela esteja em execução no modo ativo, ou a alteração da tarefa para o modo *Somente estatísticas*.

Depois de concluir uma atualização do aplicativo, recomendamos verificar as regras de Controle de Inicialização de Aplicativos migradas e sua operação no modo *Somente estatísticas*.

Migração dos valores das configurações e regras do Gerenciamento de Firewall

Durante a atualização de um aplicativo, as regras da tarefa de Gerenciamento de Firewall são migradas sem alterações.

Caso o componente Gerenciamento de Firewall não tenha sido instalado em uma versão anterior do aplicativo, após a atualização do aplicativo, a tarefa de Gerenciamento de Firewall será executada no modo de Observar o estado do Firewall do Windows.

Caso o componente Gerenciamento de Firewall tenha sido instalado em uma versão anterior do aplicativo, a tarefa Gerenciamento de Firewall será executada no modo Controlar a operação do Firewall do Windows após a atualização do aplicativo.

Atualização do aplicativo com modificação de configuração

Quando a configuração do aplicativo “Proteger o computador com bases de antivírus” é instalada pela pasta /exec sobre a versão do aplicativo que não usa análise de assinatura e bancos de dados de antivírus para proteger o computador (“Proteger o computador com a tecnologia de Negação padrão”), o conjunto de componentes do aplicativo será expandido automaticamente pela adição dos seguintes componentes:

- Proteção de Arquivos em Tempo Real
- Verificação por Demanda
- Proteção Contra Ameaças à Rede

O arquivo que contém os bancos de dados do antivírus é descompactado automaticamente.

Caso não queira usar esses componentes e tarefas para proteger o dispositivo, reinicie a instalação do aplicativo pela pasta /product_long_term.

Quando a configuração do aplicativo "Proteger o computador com a tecnologia de Negação padrão" é instalada pela pasta /product_long_term sobre a versão do aplicativo que usa análise de assinatura e bancos de dados de antivírus para proteger o computador (configuração "Proteger o computador com bases de antivírus"), o conjunto de componentes do aplicativo será reduzido automaticamente pela remoção dos seguintes componentes:

- Proteção de Arquivos em Tempo Real
- Verificação por Demanda
- os componentes que permitem atualizações

Essa configuração é recomendada para proteger dispositivos com recursos limitados. Nesse caso, você pode ativar o aplicativo por um longo período, e o componente Controle de Inicialização de Aplicativos fornece proteção ao computador.

Declaração do Kaspersky Security Network e Declaração do Kaspersky Managed Protection

Após a atualização do aplicativo para a versão 3.3, a tarefa de uso da KSN é interrompida. Para continuar usando a infraestrutura em nuvem da KSN e o serviço KMP após a atualização do aplicativo, é necessário ler e aceitar os termos da Declaração da Kaspersky Security Network e da Declaração do Kaspersky Managed Protection.

Sobre a atualização das Ferramentas de Administração do Kaspersky Embedded Systems Security for Windows

Qualquer versão do Console do Aplicativo pode ser atualizada para o Kaspersky Embedded Systems Security Console for Windows versão 3.3.

Além disso:

- Os valores de configurações do Console do Aplicativo atualizado permanecem inalterados.
- Qualquer versão anterior do Kaspersky Embedded Systems Security for Windows pode ser gerenciada pelo Console do Aplicativo versão 3.3.
- O Kaspersky Embedded Systems Security for Windows versão 3.3 pode ser gerenciado pelo Console do Aplicativo de qualquer versão anterior.

As seguintes versões do Plug-in de Administração podem ser atualizadas para a versão 3.3:

- 2.1.0.xxx;
- 2.3.0.xxx;

- 3.0.0.xxx;
- 3.1.0.xxx;
- 3.2.0.xxx.

Além disso:

- Os valores das configurações do Plug-in de Administração de qualquer versão mencionada anteriormente permanecem inalterados após uma atualização para a versão 3.3.
- As seguintes versões do Kaspersky Embedded Systems Security for Windows podem ser gerenciadas pelo Plug-in de Administração versão 3.3: 2.1.0.441, 2.3.0.754, 3.0.0.102, 3.1.0.461 e 3.2.0.200.
- O Kaspersky Embedded Systems Security for Windows versão 3.3 pode ser gerenciado pelo Plug-in de Administração de qualquer uma das versões mencionadas anteriormente.

Durante a atualização, uma nova versão do Plug-in de Administração ou do Console do Aplicativo é instalada sobre a versão instalada anteriormente e não requer a reinicialização do computador.

Códigos de componentes de software do Kaspersky Embedded Systems Security for Windows para o serviço do Windows Installer

Os arquivos \product_long_term\ess_x86.msi e \product_long_term\ess_x64.msi são projetados para instalar a configuração **Proteger o computador com tecnologia de Negação padrão** do Kaspersky Embedded Systems Security for Windows, e os arquivos \product\ess_x86.msi e \product\ess_x64.msi são projetados para instalar a configuração **Proteger o computador com bases de antivírus** do Kaspersky Embedded Systems Security for Windows.

Caso a configuração “Proteger o computador com bases de antivírus” esteja selecionada, todos os componentes do Kaspersky Embedded Systems Security for Windows serão incluídos por padrão, exceto os componentes Gerenciamento de Firewall e Contadores de Desempenho.

Quando a configuração do aplicativo “Proteger o computador com bases de antivírus” é instalada sobre a versão do aplicativo que não usa análise de assinatura e bancos de dados de antivírus para proteger o computador, o conjunto de componentes do aplicativo será expandido automaticamente pela adição dos seguintes componentes:

- Proteção de Arquivos em Tempo Real
- Verificação por Demanda
- Proteção Contra Ameaças à Rede

Os componentes que ativam atualizações não estão incluídos na configuração Proteger o computador com tecnologia de Negação padrão.

Se a configuração Proteger o computador com tecnologia de Negação padrão estiver selecionada, os seguintes componentes serão incluídos por padrão:

- Core
- Prevenção de Exploits
- Controle de Inicialização de Aplicativos
- Ícone da bandeja do sistema

Quando a configuração "Proteger o computador com a tecnologia de Negação padrão" do aplicativo é instalada sobre uma versão do aplicativo que usa análise de assinatura e bancos de dados de antivírus para proteger o computador, o conjunto de componentes do aplicativo será reduzido automaticamente pela remoção dos seguintes componentes:

- Proteção de Arquivos em Tempo Real
- Verificação por Demanda
- os componentes que permitem atualizações

Essa configuração é recomendada para proteger dispositivos com recursos limitados. Nesse caso, você pode ativar o aplicativo por um longo período, e o componente Controle de Inicialização de Aplicativos fornece proteção ao computador.

Os arquivos \console\esstools_x86.msi e \console\esstools_x64.ms instalam todos os componentes de software que são parte das Ferramentas de Administração.

As seções a seguir enumeram os códigos dos componentes do Kaspersky Embedded Systems Security for Windows 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 for Windows na linha de comando.

Componentes de software do Kaspersky Embedded Systems Security for Windows

A tabela a seguir contém códigos e descrições dos componentes de software do Kaspersky Embedded Systems Security for Windows.

Descrição dos componentes de software do Kaspersky Embedded Systems Security for Windows

Componente	Identificador	Funções do componente
Funcionalidade básica	Core	Esse componente contém o conjunto de funções básicas do aplicativo e garante sua operação. Caso outros componentes do Kaspersky Embedded Systems Security for Windows sejam especificados ao instalar o Kaspersky Embedded Systems Security for Windows a partir da linha de comando, mas o componente Core não for especificado, ele será instalado automaticamente.

Controle de Inicialização de Aplicativos	AppCtrl	Esse componente monitora as tentativas do usuário de iniciar aplicativos e permite ou nega a inicialização de aplicativos conforme as regras de Controle de Inicialização de Aplicativos especificadas. É implementado na tarefa de Controle de Inicialização de Aplicativos.
Controle de Dispositivos	DevCtrl	Esse componente rastreia as tentativas de conectar dispositivos externos a um dispositivo protegido e permite ou nega o uso desses dispositivos conforme as regras de Controle de Dispositivos especificadas. O componente é implementado na tarefa de Controle de dispositivos.
Proteção antivírus	AVProtection	Este componente fornece proteção antivírus.
Proteção Contra Ameaças à Rede	IDS	Esse componente verifica o tráfego de rede de entrada em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede direcionada ao computador, o Kaspersky Embedded Systems Security for Windows bloqueará a atividade de rede do computador invasor.
Verificação por Demanda	Ods	Esse componente instala arquivos de sistema do Kaspersky Embedded Systems Security for Windows e executa tarefas de verificação por demanda (verificação de objetos no dispositivo protegido mediante solicitação).
Proteção de Arquivos em Tempo Real	Oas	Esse componente executa verificações de vírus de arquivos no dispositivo protegido quando esses arquivos são acessados. O componente implementa a tarefa de Proteção de arquivos em tempo real.
Uso da Kaspersky Security Network	Ksn	Esse componente fornece proteção com base nas tecnologias na nuvem da Kaspersky. O componente implementa a tarefa de Uso da KSN (enviando solicitações e recebendo conclusões do serviço Kaspersky Security Network).
Monitor de Integridade de Arquivos	Fim	Esse componente registra as operações executadas em arquivos no escopo de monitoramento especificado. O componente implementa a tarefa do Monitor de Integridade de Arquivos.
Monitor de acesso ao registro	RegMonitor	Esse componente permite monitorar as ações executadas com as ramificações e chaves de registro especificadas nos escopos de monitoramento definidos nas configurações da tarefa. O componente implementa o Monitor de Acesso ao Registro.
Prevenção de Exploits	AntiExploit	Esse componente permite gerenciar as configurações para proteger a memória usada por processos na memória de um dispositivo.
Gerenciamento de Firewall	Firewall	Esse componente permite gerenciar o firewall do Windows por meio da interface gráfica do usuário do Kaspersky Embedded Systems Security for Windows. O componente implementa a tarefa de Gerenciamento de Firewall.
Módulo para integração com o Agente de Rede do Kaspersky	AKIntegration	Fornece uma conexão entre o Kaspersky Embedded Systems Security for Windows e o Agente de Rede do Kaspersky Security Center.

Security Center.		É possível instalar esse componente no dispositivo protegido, caso pretenda gerenciar o aplicativo pelo 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	Esse componente instala um conjunto de contadores de desempenho do Monitor do sistema. Os contadores de desempenho permitem que o desempenho do Kaspersky Embedded Systems Security for Windows seja medido e possíveis gargalos sejam localizados quando o Kaspersky Embedded Systems Security for Windows for usado com outros programas.
Contadores e traps SNMP	SnmpSupport	Esse componente publica contadores e traps do Kaspersky Embedded Systems Security for Windows pelo Protocolo de Gerenciamento de Rede Simples (SNMP) no Microsoft Windows. Esse componente pode ser instalado no dispositivo protegido apenas se o SNMP da Microsoft estiver instalado no mesmo dispositivo protegido.
Ícone do Kaspersky Embedded Systems Security for Windows na área de notificação	TrayApp	Esse componente exibe o ícone do Kaspersky Embedded Systems Security for Windows na área de notificação da bandeja de tarefas do dispositivo protegido. O ícone do Kaspersky Embedded Systems Security for Windows exibe o status de proteção do dispositivo e pode ser usado para abrir o Kaspersky Embedded Systems Security for Windows Console no Console de Gerenciamento da Microsoft (caso esteja instalado) e a janela **Sobre o aplicativo**.

Componente do software "ferramentas de administração"

A tabela a seguir contém o código e a descrição do componente de software "ferramentas de administração".

Descrição do componente de software "ferramentas de administração"

Componente	Código	Funções do componente
Snap-in do Kaspersky Embedded Systems Security for Windows	MmcSnapin	Esse componente instala o snap-in do Console de Gerenciamento Microsoft por meio do Console do Kaspersky Embedded Systems Security for Windows. 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.

Modificações de sistema após a instalação do Kaspersky Embedded Systems Security for Windows

Quando o Kaspersky Embedded Systems Security for Windows e o conjunto de “Ferramentas de administração” (incluindo o Console do Aplicativo) forem instalados juntos, o serviço do Windows Installer fará as seguintes modificações no dispositivo protegido:

- As pastas do Kaspersky Embedded Systems Security for Windows são criadas no dispositivo protegido e no dispositivo no qual o Console do Aplicativo estiver instalado.

- Os serviços do Kaspersky Embedded Systems Security for Windows são registrados.
- O grupo de usuários do Kaspersky Embedded Systems Security for Windows é criado.
- Chaves do Kaspersky Embedded Systems Security for Windows são registradas no registro de sistema.
- A tarefa do sistema Kaspersky Embedded Systems Security OS Upgrade Detect, exibida no Agendador de Tarefas do Windows, é criada.

Estas modificações são descritas abaixo.

Pastas do Kaspersky Embedded Systems Security for Windows em um dispositivo protegido

Quando o Kaspersky Embedded Systems Security for Windows é instalado, as seguintes pastas são criadas em um dispositivo protegido:

- A pasta da instalação padrão do Kaspersky Embedded Systems Security for Windows, que contém os arquivos executáveis do Kaspersky Embedded Systems Security for Windows depende da arquitetura do sistema operacional. Portanto, as pastas de instalação padrão são as seguintes:
  - Para a 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 Lab\Kaspersky Embedded Systems Security
- Arquivos da Management Information Base (MIB), que contêm uma descrição dos contadores e hooks publicados pelo Kaspersky Embedded Systems Security for Windows através do protocolo SNMP:
  - %Kaspersky Embedded Systems Security%\mibs
- Versões de 64 bits dos arquivos executáveis do Kaspersky Embedded Systems Security for Windows (a pasta será criada somente durante a instalação do Kaspersky Embedded Systems Security for Windows na versão de 64 bits do Microsoft Windows):
  - %Kaspersky Embedded Systems Security%\x64
- Arquivos de serviço do Kaspersky Embedded Systems Security for Windows:
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Data
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Settings
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Dskm

  Para o Windows XP, o caminho para a pasta da Kaspersky Lab é %ALLUSERSPROFILE%\Application Data
- Arquivos com configurações para fontes de atualização:

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Update

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Update
- 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).

%ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Update\Distribution

- Logs de tarefas e log de auditoria do sistema.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Reports

- Conjunto de bancos de dados em uso.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Bases\Current

- Cópias de backup dos bancos de dados; elas serão substituídas sempre que os bancos de dados forem atualizados.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Bases\Backup

- Arquivos temporários criados durante a execução das tarefas de atualização.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Bases\Temp

- Objetos na Quarentena (pasta padrão).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Quarantine

- Objetos no backup (pasta padrão).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Backup

- Objetos restaurados do backup e da quarentena (pasta padrão para objetos restaurados).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Restored

Pastas criadas durante a instalação do Console do Aplicativo

As pastas de instalação padrão do Console do Aplicativo que contém os arquivos de "Ferramentas de administração" dependem da arquitetura do sistema operacional. Portanto, as pastas de instalação padrão são as seguintes:

- Para a versão de 32 bits do Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

- Para a versão de 64 bits do Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

Serviços do Kaspersky Embedded Systems Security for Windows

Os serviços do Kaspersky Embedded Systems Security for Windows a seguir são inicializados utilizando a conta do sistema local (SYSTEM):

- Kaspersky Security Service (KAVFS) – serviço essencial do Kaspersky Embedded Systems Security for Windows que gerencia tarefas e fluxos de trabalho do Kaspersky Embedded Systems Security for Windows.

- Kaspersky Security Management Service (KAVFSGT) – este serviço é destinado ao gerenciamento de aplicativos do Kaspersky Embedded Systems Security for Windows por meio do Console do Aplicativo.

- Serviço de Kaspersky Security Exploit Prevention (KAVFSSLP) – esse serviço funciona como um intermediário para comunicar as configurações de segurança aos agentes de segurança externos e para receber dados sobre eventos de segurança.

Grupo Kaspersky Embedded Systems Security for Windows

Administradores de ESS é um grupo no dispositivo protegido cujos usuários possuem acesso total ao Kaspersky Security Management Service e a todas as funções do Kaspersky Embedded Systems Security.

Chaves do registro do sistema

Quando o Kaspersky Embedded Systems Security for Windows é instalado, as seguintes chaves do registro do sistema são criadas:

- Propriedades do Kaspersky Embedded Systems Security for Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Configurações de log de eventos do Kaspersky Embedded Systems Security for Windows (Log de Eventos Kaspersky): [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Propriedades do serviço de gerenciamento do Kaspersky Embedded Systems Security for Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Configurações dos contadores de desempenho:
  - Para a versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - Para a versão de 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Configurações do componente de Suporte do Protocolo SNMP:
  - Para a versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\SnmpAgent]
  - Para a versão 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3\SnmpAgent]
- Configurações do arquivo de despejo:
  - Para a versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\CrashDump]
  - Para a versão 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3\CrashDump]
- Configurações do arquivo de rastreamento:
  - Para a versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\Trace]
  - Para a versão 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3\Trace]
- Configurações para tarefas e funções do aplicativo: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3\Environment]

Tarefa do sistema Kaspersky Embedded Systems Security OS Upgrade Detect

O serviço Windows Installer cria uma tarefa Kaspersky Embedded Systems Security OS Upgrade Detect durante a instalação do aplicativo. A tarefa é iniciada imediatamente após sua criação e posteriormente a cada inicialização do SO. A tarefa verifica a versão dos drivers usados pelo aplicativo: caso uma versão do sistema operacional seja atualizada, o aplicativo atualizará os drivers para a versão correspondente do sistema operacional.

A tarefa não afeta o aplicativo e pode ser excluída. Recomendamos manter o cenário de atualização do sistema operacional em mente.

Processos do Kaspersky Embedded Systems Security for Windows

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

Processos do Kaspersky Embedded Systems Security for Windows

Nome do arquivo	Finalidade
kavfswp.exe	Fluxo de trabalho do Kaspersky Embedded Systems Security for Windows
kavtray.exe	Processo para ícone de bandeja do sistema
kavfsmui.exe	Processo do componente de Interface de diagnóstico compacta
kavshell.exe	Processo do utilitário de linha de comando
kavfsrcn.exe	Processo de gerenciamento remoto do Kaspersky Embedded Systems Security for Windows
kavfs.exe	Processo do Kaspersky Security Service
kavfsgt.exe	Processos do Kaspersky Security Management Service
kavfswh.exe	Processo do Serviço de Kaspersky Security Exploit Prevention

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

Esta seção contém descrições das configurações para a instalação e desinstalação do Kaspersky Embedded Systems Security for Windows, seus valores padrão, chaves para alterar as configurações de instalação e seus possíveis valores. 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 for Windows a partir da linha de comando.

Configurações de instalação e opções da linha de comando no Windows Installer

- Aceitação dos termos do Contrato de Licença do Usuário Final: você deve aceitar os termos para instalar o Kaspersky Embedded Systems Security for Windows.

  Os valores possíveis para a opção `EULA=<value>` na linha de comando são os seguintes:

  - `0` – você não aceita os termos do Contrato de Licença do Usuário Final (valor padrão).

- `1` – você aceita os termos do Contrato de licença do usuário final.

- Aceitação dos termos da Política de Privacidade: você deve aceitar os termos para instalar o Kaspersky Embedded Systems Security for Windows.

  Os valores possíveis para a opção `PRIVACYPOLICY=<value>` na linha de comando são os seguintes:

  - `0` – você não aceita os termos da Política de Privacidade (valor padrão).

  - `1` – você aceita os termos da Política de Privacidade.

- Permitir a instalação do Kaspersky Embedded Systems Security for Windows se a atualização KB4528760 não estiver instalada. Para obter informações detalhadas sobre a atualização KB4528760, visite o site da Microsoft.

  Os valores possíveis para a opção de linha de comando `SKIPCVEWINDOWS10=<valor>` são os seguintes:

  - `0` – cancele a instalação do Kaspersky Embedded Systems Security for Windows se a atualização KB4528760 não estiver instalada (valor padrão).

  - `1` – permita a instalação do Kaspersky Embedded Systems Security for Windows se a atualização KB4528760 não estiver instalada.

  A atualização KB4528760 corrige a vulnerabilidade de segurança CVE-2020-0601. Para obter informações detalhadas sobre a vulnerabilidade de segurança CVE-2020-0601, visite o site da Microsoft.

- Instalação do Kaspersky Embedded Systems Security for Windows com preservação das configurações da versão anterior durante a atualização.

  Os valores possíveis para a opção RESTOREDEFSETTINGS=<valor> na linha de comando são:

  - `0` – todos os dados da versão anterior são migrados para uma nova versão durante a atualização (valor padrão).

  - `1` – apenas o arquivo com os dados de ativação e as chaves privadas é migrado para uma nova versão durante a atualização ([unidade]:\ProgramData\Kaspersky Lab\<produto>\<versão>\Data\product.dat). Todos os outros dados da versão anterior, como configurações, bancos de dados de antivírus, relatórios, objetos de quarentena e backup são excluídos.

- Instalação do Kaspersky Embedded Systems Security for Windows com preservação dos relatórios de versões anteriores durante a atualização.

  Os valores possíveis para a opção KEEP_REPORTS=<valor> na linha de comando são:

  - `0` – todos os dados da versão anterior, exceto os relatórios ([unidade]:\ProgramData\Kaspersky Lab\<produto>\<versão>\Reports), são migrados para a nova versão durante a atualização. Os relatórios são excluídos.

  - `1` – todos os dados da versão anterior, como configurações, bancos de dados de antivírus, relatórios, objetos de quarentena e backup são migrados para uma nova versão durante a atualização (valor padrão).

- Instalação do Kaspersky Embedded Systems Security for Windows com uma verificação preliminar dos processos ativos e setores de inicialização dos discos locais.

  Os valores possíveis para a opção `PRESCAN=<valor>` na linha de comando são os seguintes:

  - `0` – não executar uma verificação preliminar de processos ativos e setores de inicialização de discos locais durante a instalação (valor padrão).

- `1` – executar uma verificação preliminar de processos ativos e setores de inicialização de discos locais durante a instalação.

- Pasta de destino onde os arquivos do Kaspersky Embedded Systems Security for Windows serão salvos durante a instalação. Uma pasta diferente pode ser especificada.

  Os valores padrão da opção `INSTALLDIR=<caminho completo para a pasta>` na linha de comando são os seguintes:

  - Kaspersky Embedded Systems Security for Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - Ferramentas de administração: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
  - Na versão de 64 bits do Microsoft Windows: %ProgramFiles(x86)%

- O início da tarefa de Proteção de Arquivos em Tempo Real acontece imediatamente após a inicialização do Kaspersky Embedded Systems Security for Windows.

  Os valores possíveis para a opção `RUNRTP=< valor >` na linha de comando são os seguintes:

  - `1` – iniciar (valor padrão).
  - `0` – não iniciar.

- Modo de execução para a tarefa Proteção de Arquivos em Tempo Real.

  Os valores possíveis para a opção `RUNRTP=< valor >` na linha de comando são os seguintes:

  - `1` – Recomendado (valor padrão).
  - `0` – Somente notificações.

- Objetos excluídos do escopo da proteção segundo as recomendações da Microsoft Corporation. Na tarefa Proteção de Arquivos em Tempo Real, exclua do escopo da proteção objetos no dispositivo que sejam recomendados para exclusão pela Microsoft Corporation. Alguns aplicativos no dispositivo protegido podem ficar instáveis quando o aplicativo antivírus intercepta ou modifica arquivos usados por eles. Por exemplo, a Microsoft Corporation inclui alguns aplicativos de controladores de domínio na lista de tais objetos.

  Os valores possíveis para a opção `ADDMSEXCLUSION=<valor>` na linha de comando são os seguintes:

  - `1` – excluir (valor padrão).
  - `0` – não excluir.

- Objetos excluídos do escopo da proteção segundo as recomendações da Kaspersky. Na tarefa Proteção de Arquivos em Tempo Real, exclua do escopo da proteção objetos no dispositivo que sejam recomendados para exclusão pela Kaspersky.

  Os valores possíveis para a opção `ADDKLEXCLUSION=<valor>` na linha de comando são os seguintes:

  - `1` – excluir (valor padrão).
  - `0` – não excluir.

- Permitir a conexão remota ao Console do Aplicativo. Por padrão, a conexão remota com o Console do Aplicativo instalado no dispositivo protegido não é permitida. Durante a instalação, você pode permitir a conexão. O Kaspersky Embedded Systems Security for Windows cria regras de permissão para o processo kavfsgt.exe usando o protocolo TCP para todas as portas.

Os valores possíveis para a opção `ALLOWREMOTECON=<valor>` na linha de comando são os seguintes:

- `1` – permitir.
- `0` – negar (valor padrão).

- Caminho para o arquivo de chave (`LICENSEKEYPATH`). Por padrão, o Windows Installer tenta encontrar o arquivo com a extensão .key na pasta \exec do kit de distribuição. Caso a pasta \exec contenha vários arquivos de chave, o Windows Installer selecionará o arquivo de chave cuja data de expiração seja a mais distante no futuro. Um arquivo de chave pode ser salvo antecipadamente na pasta \exec ou pela especificação de outro caminho para o arquivo de chave com o uso da configuração **Adicionar chave**. É possível adicionar uma chave depois que o Kaspersky Embedded Systems Security for Windows tiver sido 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 for Windows não funcionará.

- Caminho do arquivo de configuração. O Kaspersky Embedded Systems Security for Windows importa configurações do arquivo de configuração especificado criado no aplicativo. O Kaspersky Embedded Systems Security for Windows 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.

  O valor padrão de `CONFIGPATH=<nome do arquivo de configuração>` não é especificado.

- Modo da tarefa **Verificação na Inicialização do Sistema Operacional** (SCANSTARTUP_BLOCKING). Caso o Kaspersky Embedded Systems Security for Windows tenha sido instalado no modo de instalação sem a chave SCANSTARTUP_BLOCKING, a tarefa **Verificação na Inicialização do Sistema Operacional** terá os seguintes parâmetros atribuídos na configuração do **Escopo de verificação**:

  - **Ação a ser executada em objetos infectados e outros: Apenas notificar**
  - **Ação a ser executada em objetos possivelmente infectados: Apenas notificar**

  Caso o Kaspersky Embedded Systems Security for Windows tenha sido instalado no modo de instalação com o uso da chave SCANSTARTUP_BLOCKING, a tarefa **Verificação na Inicialização do Sistema Operacional** terá os seguintes parâmetros atribuídos na configuração do **Escopo de verificação**:

  - **Ação a ser executada em objetos infectados e outros: Executar a ação recomendada**
  - **Ação a ser executada em objetos possivelmente infectados: Executar a ação recomendada**

  A tarefa **Verificação na Inicialização do Sistema Operacional** é criada automaticamente. Por padrão, o modo **Apenas notificar** é aplicado. Nesse caso, depois de implementar o Kaspersky Embedded Systems Security for Windows nos dispositivos, será possível ativar a tarefa **Verificação na Inicialização do Sistema Operacional** caso nenhum problema com os serviços do sistema tenha sido descoberto durante a verificação. Caso o aplicativo detecte serviços críticos do sistema como objetos infectados ou provavelmente infectados, o modo **Apenas notificação** dará tempo para descobrir o motivo e resolver o problema. Se o aplicativo aplicar o modo **Executar ação recomendada**, que chama o método **Desinfetar.** Ação **Remover se a desinfecção falhar**. A desinfecção ou remoção dos arquivos do sistema pode resultar em problemas críticos com a inicialização do sistema operacional.

- A ativação das conexões de rede para a opção Console do Aplicativo é usada para instalar o Console do Kaspersky Embedded Systems Security for Windows em outro dispositivo. É possível gerenciar remotamente a proteção de um dispositivo a partir de outro dispositivo com o Console do Kaspersky Embedded Systems Security for Windows 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 for Windows e o acesso é concedido aos aplicativos DCOM. Após a conclusão da instalação, adicione usuários ao grupo Administradores de ESS para que possam gerenciar remotamente o aplicativo e permitir conexões de rede ao Kaspersky Security Management Service (arquivo kavfsgt.exe) no

dispositivo protegido. Você pode ler mais sobre as configurações adicionais quando o Console do Kaspersky Embedded Systems Security for Windows estiver instalado em outro dispositivo.

Os valores possíveis para a opção `ADDWFEXCLUSION=<valor>` na linha de comando são os seguintes:

- `1` – permitir.
- `0` – negar (valor padrão).

- Desativação da verificação de software incompatível. Use essa configuração para ativar ou desativar a verificação de software incompatível durante a instalação em segundo plano do aplicativo no dispositivo protegido. Independentemente do valor dessa configuração, durante a instalação do Kaspersky Embedded Systems Security for Windows, o aplicativo sempre avisará sobre outras versões do aplicativo instaladas no dispositivo protegido.

  Os valores possíveis para a opção `SKIPINCOMPATIBLESW=<valor>` na linha de comando são os seguintes:

  - `0` - A verificação de software incompatível é realizada (valor padrão).
  - `1` - A verificação de software incompatível não é realizada.

Configurações de desinstalação e opções de linha de comando no Windows Installer

- Restauração de objetos da quarentena.

  Os valores possíveis para a opção `RESTOREQTN=<valor>` na linha de comando são os seguintes:

  - `0` – remover o conteúdo em quarentena (valor padrão).
  - `1` – restaurar o conteúdo em quarentena para a pasta especificada pelo parâmetro RESTOREPATH na subpasta \Quarantine.

- Restauração do conteúdo do backup.

  Os valores possíveis para a opção `RESTOREBCK=<valor>` na linha de comando são os seguintes:

  - `0` – remover o conteúdo do backup (valor padrão).
  - `1` – restaurar o conteúdo do backup para a pasta especificada pelo parâmetro RESTOREPATH na subpasta \Backup.

- Insira a senha atual para confirmar a desinstalação (se a proteção de senha estiver ativa).

  O valor padrão de `UNLOCK_PASSWORD=<senha especificada>` não é especificado.

- Pasta para a objetos restaurados. Objetos restaurados serão salvos na pasta especificada.

  O valor padrão para a opção `RESTOREPATH=<caminho completo para a pasta>` na linha de comando é %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Restored

Logs de instalação e desinstalação do Kaspersky Embedded Systems Security for Windows

Se o Kaspersky Embedded Systems Security for Windows for instalado ou desinstalado usando o Assistente de instalação (Desinstalação), o serviço do Windows Installer cria um log de instalação (desinstalação). Um arquivo de log nomeado ess_v3.3_install_<uid>.log (onde <uid> é um identificador de log único de 8 caracteres) será salvo na pasta %temp% do usuário cuja conta foi usada para executar o arquivo setup.exe.

Caso execute a opção **Modificar ou remover** para o Console do Aplicativo ou para o Kaspersky Embedded Systems Security for Windows pelo menu **Iniciar**, um arquivo de log chamado ess_v3.3_install_<uid> será criado automaticamente na pasta %temp%.

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

Para instalar o Kaspersky Embedded Systems Security for Windows e criar o arquivo de log 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 descreve o conjunto de ferramentas de administração do Kaspersky Embedded Systems Security for Windows e os aspectos especiais da instalação e desinstalação do Kaspersky Embedded Systems Security for Windows usando um assistente, a linha de comando, o Kaspersky Security Center e uma política de grupo do Active Directory.

Antes de iniciar a instalação do Kaspersky Embedded Systems Security for Windows, planeje as etapas principais.

1. Determine que ferramentas de administração serão usadas para gerenciar e configurar o Kaspersky Embedded Systems Security for Windows.
2. Selecione os componentes do aplicativo necessários para instalação.
3. Selecione o método de instalação.

Seleção das ferramentas de administração

Determine as ferramentas de administração que serão usadas para configurar e gerenciar o Kaspersky Embedded Systems Security for Windows. O Kaspersky Embedded Systems Security for Windows 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 for Windows

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

Vários snap-ins do Kaspersky Embedded Systems Security for Windows podem ser adicionados a um Console de Gerenciamento Microsoft aberto no modo autor para gerenciar a proteção de vários dispositivos nos quais o Kaspersky Embedded Systems Security for Windows esteja instalado.

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

Utilitário de linha de comando

É possível gerenciar o Kaspersky Embedded Systems Security for Windows a partir da linha de comando de um dispositivo protegido.

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

Kaspersky Security Center

Se o aplicativo do Kaspersky Security Center for usado para o gerenciamento centralizado da proteção antivírus de dispositivos na sua empresa, você poderá gerenciar o Kaspersky Embedded Systems Security for Windows 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 for Windows. Ele permite a comunicação do Kaspersky Embedded Systems Security for Windows com o Agente de Rede. Instale o módulo para a integração com o Agente de Rede do Kaspersky Security Center no dispositivo protegido.

- **Agente de Rede do Kaspersky Security Center**. Instale este componente em cada dispositivo protegido. Esse componente suporta a interação entre o Kaspersky Embedded Systems Security for Windows instalado no dispositivo protegido 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 3.3 for Windows**. Adicionalmente, instale o Plug-in de Administração para gerenciar o Kaspersky Embedded Systems Security for Windows por meio do Console de Administração no dispositivo protegido no qual Servidor de Administração do Kaspersky Security Center está instalado. Ele fornece a interface de gerenciamento de aplicativos por meio do Kaspersky Security Center. O arquivo de instalação do Plug-in de Administração, \exec\klcfginst.exe, está incluído no kit de distribuição do Kaspersky Embedded Systems Security for Windows.

Seleção do tipo de instalação

Depois de especificar os componentes do software para instalação do Kaspersky Embedded Systems Security for Windows, selecione o método de instalação do aplicativo.

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

- Se precisar de configurações de instalação do Kaspersky Embedded Systems Security for Windows especiais ou das configurações de instalação recomendadas.

- Se as configurações de instalação forem as mesmas para todos os dispositivos protegidos ou específicas para cada um deles.

O Kaspersky Embedded Systems Security for Windows pode ser instalado interativamente usando o Assistente de instalação ou em modo silencioso sem a participação do usuário, e pode ser chamado executando o arquivo do pacote de instalação com as configurações de instalação a partir da linha de comando. Uma instalação remota centralizada do Kaspersky Embedded Systems Security for Windows 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 for Windows pode ser instalado e configurado em um único dispositivo protegido com suas configurações salvas em um arquivo de configuração; o arquivo criado pode então ser usado para instalar o Kaspersky Embedded Systems Security for Windows em outros dispositivos protegidos. Observe que essa possibilidade não existe quando o produto é instalado usando as políticas de grupo do Active Directory.

Inicialização do assistente de instalação

O assistente de instalação pode instalar o seguinte:

- Componentes do Kaspersky Embedded Systems Security for Windows em um dispositivo protegido fora de um arquivo \exec\setup.exe incluído no kit de distribuição.
- O Console do Kaspersky Embedded Systems Security for Windows do arquivo \console\setup.exe no kit de distribuição do dispositivo protegido ou em outro host da 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 for Windows será instalado com a configuração padrão. As opções especiais do Kaspersky Embedded Systems Security for Windows podem ser usadas para modificar as configurações de instalação.

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

Você também pode usar exemplos de comandos para a instalação do Kaspersky Embedded Systems Security for Windows e do Console do Aplicativo.

Instalação centralizada por meio do Kaspersky Security Center

Se o Kaspersky Security Center for usado para gerenciamento da proteção antivírus dos dispositivos na sua rede, o Kaspersky Embedded Systems Security for Windows poderá ser instalado em vários dispositivos usando a tarefa de instalação remota.

Os dispositivos protegidos nos quais você deseja instalar o Kaspersky Embedded Systems Security for Windows por meio do Kaspersky Security Center podem estar localizados no mesmo domínio do Kaspersky Security Center, 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 for Windows no dispositivo protegido. O Console do Aplicativo pode ser instalado no dispositivo protegido ou na estação de trabalho do administrador.

O Kaspersky Embedded Systems Security for Windows pode ser instalado usando somente as configurações de instalação recomendadas.

Os dispositivos protegidos nos quais o Kaspersky Embedded Systems Security for Windows está instalado usando as políticas de grupo do Active Directory devem estar localizados no mesmo domínio e na mesma unidade organizacional. A instalação é realizada na inicialização do dispositivo protegido, antes de fazer login no Microsoft Windows.

Instalação e desinstalação do aplicativo usando um assistente

Esta seção descreve a instalação e desinstalação do Kaspersky Embedded Systems Security for Windows e do Console do Aplicativo por meio do assistente de instalação e contém informações sobre as configurações adicionais do Kaspersky Embedded Systems Security for Windows e ações a serem executadas após a instalação.

Instalação usando o Assistente de instalação

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

Para instalar e prosseguir com a utilização do Kaspersky Embedded Systems Security for Windows:

1. Instale o Kaspersky Embedded Systems Security for Windows no dispositivo protegido.
2. Instale o Console do Aplicativo nos dispositivos a partir dos quais pretende gerenciar o Kaspersky Embedded Systems Security for Windows.
3. Caso o Console do Aplicativo tenha sido instalado em qualquer dispositivo na rede além do dispositivo protegido, execute a configuração adicional para permitir que usuários do Console do Aplicativo gerenciem remotamente o Kaspersky Embedded Systems Security for Windows.
4. Realize ações após a instalação do Kaspersky Embedded Systems Security for Windows.

Instalação do Kaspersky Embedded Systems Security for Windows

Antes de instalar o Kaspersky Embedded Systems Security for Windows, faça o seguinte:

1. Certifique-se de que nenhum outro programa antivírus esteja instalado no dispositivo protegido.
2. Verifique e confirme se a conta usada para executar o assistente de instalação faz parte do grupo de administradores no dispositivo protegido.

Após concluir as ações descritas acima, prossiga com o procedimento de instalação. Especifique as configurações para instalação do Kaspersky Embedded Systems Security for Windows de acordo com as instruções do Assistente de instalação. O processo de instalação do Kaspersky Embedded Systems Security for Windows 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).

Para instalar o Kaspersky Embedded Systems Security for Windows usando o assistente de instalação:

1. Execute o arquivo setupui.exe no dispositivo protegido.

2. Na janela aberta, na seção **Instalação**, clique no link **Proteger o computador com tecnologia de Negação padrão** ou **Proteger o computador com bases de antivírus**.

Caso a configuração "Proteger o computador com bases de antivírus" esteja selecionada, todos os componentes do Kaspersky Embedded Systems Security for Windows serão incluídos por padrão, exceto os componentes Gerenciamento de Firewall e Contadores de Desempenho.

Quando a configuração do aplicativo "Proteger o computador com bases de antivírus" é instalada sobre a versão do aplicativo que não usa análise de assinatura e bancos de dados de antivírus para proteger o computador, o conjunto de componentes do aplicativo será expandido automaticamente pela adição dos seguintes componentes:

- Proteção de Arquivos em Tempo Real
- Verificação por Demanda
- Proteção Contra Ameaças à Rede

Os componentes que ativam atualizações não estão incluídos na configuração Proteger o computador com tecnologia de Negação padrão.

Se a configuração Proteger o computador com tecnologia de Negação padrão estiver selecionada, os seguintes componentes serão incluídos por padrão:

- Core
- Prevenção de Exploits
- Controle de Inicialização de Aplicativos
- Ícone da bandeja do sistema

Quando a configuração "Proteger o computador com a tecnologia de Negação padrão" do aplicativo é instalada sobre uma versão do aplicativo que usa análise de assinatura e bancos de dados de antivírus para proteger o computador, o conjunto de componentes do aplicativo será reduzido automaticamente pela remoção dos seguintes componentes:

- Proteção de Arquivos em Tempo Real
- Verificação por Demanda
- os componentes que permitem atualizações

Essa configuração é recomendada para proteger dispositivos com recursos limitados. Nesse caso, você pode ativar o aplicativo por um longo período, e o componente Controle de Inicialização de Aplicativos fornece proteção ao computador.

3. Na tela de boas-vindas do Assistente de instalação do Kaspersky Embedded Systems Security for Windows, clique no botão **Avançar**.

   A janela **Contrato de Licença do Usuário Final e Política de Privacidade** é exibida.

4. Revise os termos do Contrato de Licença e da Política de Privacidade.

5. Caso concorde com os termos e condições do Contrato de Licença do Usuário Final e da Política de Privacidade, marque as caixas de seleção **Confirmo que li completamente, entendi e aceito os termos e condições deste Contrato de Licença do Usuário Final** e marque as caixas de seleção **Estou ciente e**

concordo que meus dados serão manuseados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade. Confirmo que li completamente e entendi a Política de Privacidade para prosseguir com a instalação.

Se você não aceitar o Contrato de Licença do Usuário Final 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.

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

8. Para cancelar todas as alterações, clique no botão **Instalação personalizada** na janela **Redefinir**. Clique no botão **Avançar**.

9. Na janela **Selecionar uma pasta de destino**:

   - Se necessitado, especifique uma pasta à qual os arquivos do Kaspersky Embedded Systems Security for Windows 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 de arquivos em tempo real após a instalação do aplicativo (recomendado)**
    - **Adicionar arquivos recomendados pela Microsoft à lista de exclusões**
    - **Adicionar arquivos recomendados pela Kaspersky à lista de exclusões**

      Clique no botão **Avançar**.

11. Na janela **Importar configurações do arquivo de configuração**:

    a. Especifique o arquivo de configuração do qual importar as configurações do Kaspersky Embedded Systems Security for Windows a partir de um arquivo de configuração existente criado em qualquer versão anterior compatível do aplicativo.

    b. Clique no 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 for Windows para a ativação do aplicativo.
    - Se quiser ativar o aplicativo mais tarde, pressione o botão **Avançar**.

- Caso um arquivo de chave tenha sido salvo anteriormente na pasta \exec do kit de distribuição, o nome desse arquivo será exibido no campo **Chave**.

  Para adicionar uma chave usando um 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 for Windows exibirá a data calculada da expiração da licença. O período da licença inicia no momento em que você adiciona uma chave e expira até a data de expiração do arquivo de chave.

  Clique no botão **Avançar** para aplicar o arquivo de chave ao aplicativo.

13. Na janela **Pronto para instalar**, clique no botão **Instalar**. O assistente iniciará a instalação dos componentes do Kaspersky Embedded Systems Security for Windows.

14. A janela **Instalação concluída** será exibida quando a instalação for concluída.

15. Clique no botão **Concluir**.

O Assistente de instalação será fechado. Após a conclusão da instalação, o Kaspersky Embedded Systems Security for Windows estará pronto para uso se você tiver adicionado a chave de ativação.

Instalação do Console do Kaspersky Embedded Systems Security for Windows

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:

1. Certifique-se de que a conta utilizada para executar o Assistente de instalação faça parte do grupo de administradores no dispositivo.

2. Execute o arquivo setupui.exe no dispositivo protegido.

   A janela de boas-vindas é exibida.

3. Clique no link **Instalar o console do Kaspersky Embedded Systems Security for Windows**.

   A janela de boas-vindas do Assistente de instalação é exibida.

4. Clique no botão **Avançar**.

5. Na janela, revise os termos do Contrato de Licença do Usuário Final e da Política de Privacidade e marque as caixas de seleção com a legenda **Confirmo que li, entendi e aceitei completamente os termos e condições deste Contrato de Licença do Usuário Final** para continuar com a instalação.

6. Clique no botão **Avançar**.

   A janela **Configurações avançadas de instalação** é exibida.

7. Na janela **Configurações avançadas de instalação**:

- Se você pretende usar o Console do Aplicativo para gerenciar o Kaspersky Embedded Systems Security for Windows instalado em um dispositivo 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 de "Ferramentas de administração" a partir da lista.

  Por padrão, todos os componentes são instalados.

  c. Clique no botão **Avançar**.

Você pode encontrar informações mais detalhadas sobre os componentes do Kaspersky Embedded Systems Security for Windows.

8. Na janela **Selecionar uma pasta de destino**:

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

   b. Clique no botão **Avançar**.

9. Na janela **Pronto para instalar**, clique no botão **Instalar**.

   O assistente começará a instalação dos componentes selecionados.

10. Clique no botão **Concluir**.

O Assistente de instalação será fechado. O Console do Aplicativo será instalado no dispositivo protegido.

Caso o conjunto de “Ferramentas de Administração” tenha sido instalado em qualquer dispositivo da rede que não seja o dispositivo protegido, defina as configurações avançadas.

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

Se o Console do Aplicativo tiver sido instalado em algum dispositivo na rede além do dispositivo protegido, execute as seguintes ações para permitir que os usuários gerenciem o Kaspersky Embedded Systems Security for Windows remotamente:

- Adicione usuários do Kaspersky Embedded Systems Security for Windows ao grupo Administradores do ESS no dispositivo protegido.
- Permita conexões de rede para o Kaspersky Security Management Service (kavfsgt.exe) se o dispositivo protegido usar o Firewall do Windows ou um firewall de terceiros.
- Se a caixa de seleção **Permitir acesso remoto** não for marcada durante a instalação do Console do Aplicativo em um dispositivo com Microsoft Windows, permita conexões de rede para o Console do Aplicativo manualmente por meio do Firewall do dispositivo.

O Console do Aplicativo no dispositivo remoto usa o protocolo DCOM para receber informações sobre eventos do Kaspersky Embedded Systems Security for Windows (como objetos verificados, tarefas concluídas, etc.) do Kaspersky Security Management Service no dispositivo 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 dispositivo remoto em que 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 for Windows, kavfsrcn.exe.

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

  Diferentemente dos serviços TCP/IP e UDP/IP tradicionais, em que um protocolo único tem uma porta fixa, o DCOM atribui portas dinamicamente aos objetos COM remotos. Se existir um firewall entre o cliente (onde o Console do Aplicativo está instalado) e o ponto de extremidade do DCOM (o dispositivo protegido), um grande intervalo de portas deverá ser aberto.

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

Se o Console do Aplicativo estiver aberto enquanto você configura a conexão entre o dispositivo protegido e o dispositivo no qual o Console do Aplicativo está instalado:

1. Feche o Console do Aplicativo.
2. Espere até que o processo de gerenciamento remoto do Kaspersky Embedded Systems Security for Windows tenha terminado.
3. Reiniciar o Console do Aplicativo.

   As novas configurações de conexão serão aplicadas.

Permitir o acesso remoto anônimo a aplicativos COM

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

Para permitir o acesso remoto anônimo a aplicativos COM:

1. No dispositivo remoto com o Console do Kaspersky Embedded Systems Security for Windows instalado, abra o console de Serviços do componente.
2. Selecione **Iniciar** → **Executar**.
3. Digite o comando `dcomcnfg`.
4. Clique no botão **OK**.

5. Expanda o node **Computadores** no console de **Serviços do componente** em seu dispositivo protegido.
6. Abra o menu de contexto no node **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 no botão **OK**.

Permitir conexões de rede para o processo de gerenciamento remoto do Kaspersky Embedded Systems Security for Windows

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

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

1. Feche o Console do Kaspersky Embedded Systems Security for Windows no dispositivo remoto.
2. Execute uma das seguintes ações:
   - No Microsoft Windows XP SP2 ou posterior:
     a. Selecione **Iniciar** > **Firewall do Windows**.
     b. Na janela do **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 for Windows DCOM, e especifique o número da porta (135) no campo **Nome da porta**.
     d. Selecione o protocolo **TCP**.
     e. Clique no botão **OK**.
     f. Clique no botão **Adicionar** na guia **Exclusões**.
   - No Microsoft Windows 7 ou posterior:
     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 se 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 for Windows usando o Console de Gerenciamento Microsoft.

4. Clique no botão **OK**.

5. Clique no botão **OK** na janela **Firewall do Windows (Configurações do Firewall do Windows)**.

Adicionar regra de saída no Firewall do Windows

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

Para adicionar a regra de saída para o 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 node secundário **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 for Windows

O Kaspersky Embedded Systems Security for Windows iniciará as tarefas de proteção e verificação imediatamente após a instalação se o aplicativo tiver sido ativado. Se a opção **Ativar a proteção de arquivos em tempo real após a instalação do aplicativo (recomendado)** (opção padrão) tiver sido selecionada durante a instalação do Kaspersky Embedded Systems Security for Windows, o aplicativo verificará os objetos do sistema de arquivos do dispositivo quando eles forem acessados. O Kaspersky Embedded Systems Security for Windows 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 for Windows:

- Inicie a tarefa Atualização do Banco de Dados do aplicativo. Após a instalação, o Kaspersky Embedded Systems Security for Windows 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 for Windows 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 dispositivo se nenhum software antivírus com proteção de arquivos em tempo real estiver instalado no dispositivo antes da instalação do Kaspersky Embedded Systems Security for Windows.

- Configure notificações de administrador sobre eventos do Kaspersky Embedded Systems Security for Windows.

Inicialização e configuração da tarefa de atualização do banco de dados do Kaspersky Embedded Systems Security for Windows

Para atualizar o banco de dados do aplicativo após a instalação:

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

2. Inicie a tarefa de Atualização do Banco de Dados.

O Web Proxy Auto-Discovery Protocol (WPAD) pode não estar configurado na sua rede para detectar as configurações do servidor proxy automaticamente na LAN. Nesse caso, a sua rede pode requerer autenticação para acessar o servidor proxy.

Para especificar as configurações opcionais do servidor proxy e de autenticação para acesso ao servidor proxy:

1. Abra o menu de contexto do node **Kaspersky Embedded Systems Security for Windows**.

2. Selecione **Propriedades**.

   A janela **Configurações do aplicativo** é exibida.

3. Selecione a guia **Configurações de conexão**.

4. Na seção **Configurações do servidor proxy**, marque a caixa de seleção **Usar o servidor proxy especificado**.

5. Insira o endereço do servidor proxy no campo **Endereço** e insira o número da porta do servidor proxy no campo **Porta**.

6. Na seção **Configurações de autenticação do servidor proxy**, selecione o método de autenticação necessário na lista suspensa:

   - **Usar autenticação NTLM** se o servidor proxy suportar a autenticação NTLM integrada do Microsoft Windows. O Kaspersky Embedded Systems Security for Windows usará a conta especificada nas configurações da tarefa para acessar o servidor proxy. Por padrão, a tarefa é iniciada na conta **Sistema local** (**SYSTEM**).

- **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 for Windows 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 do aplicativo**.

Para configurar a conexão com os servidores de atualização da Kaspersky, 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 dispositivo protegido. Para isso, selecione **Iniciar**> **Todos os Programas** > **Kaspersky Embedded Systems Security for Windows** > **Ferramentas de Administração** > **Console do Kaspersky Embedded Systems Security 3.3 for Windows**.

   - Se o Console do Aplicativo tiver sido iniciado em um dispositivo diferente do dispositivo protegido, conecte-se ao dispositivo:

     a. Abra o menu de contexto do node **Kaspersky Embedded Systems Security for Windows** na árvore do Console do Aplicativo.

     b. Selecione o item **Conectar a outro computador**.

     c. Na caixa de diálogo **Selecionar dispositivo protegido**, selecione **Outro dispositivo** e, no campo de texto, indique o nome da rede do dispositivo protegido.

     Se a conta usada para entrar no Microsoft Windows não tiver permissões de acesso ao Kaspersky Security Management Service, indique uma com as permissões necessárias.

   A janela do Console do Aplicativo é exibida.

2. Na árvore do Console do Aplicativo, expanda o node **Atualização**.

3. Selecionar o node secundário **Atualização do Banco de Dados**.

4. Clique no link **Propriedades** no painel de resultados.

5. Na janela **Configurações de tarefa** exibida, abra a guia **Configurações de conexão**.

6. Selecione **Usar configurações do servidor proxy para conectar aos servidores de atualização da Kaspersky**.

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 node **Atualização**.

2. No menu de contexto no node secundário **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, é possível visualizar a data de lançamento das últimas atualizações do banco de dados instaladas no painel de resultados do node **Kaspersky Embedded Systems Security for Windows**.

Verificação de Áreas Críticas

Após ter atualizado os bancos de dados do Kaspersky Embedded Systems Security for Windows, verifique o dispositivo protegido quanto à presença de malware usando a tarefa de Verificação de áreas críticas.

Para executar a tarefa de Verificação de Áreas Críticas:

1. Expanda o node **Verificação por demanda** na árvore do Console do Aplicativo.
2. No menu de contexto do node secundário **Verificação de Áreas Críticas**, selecione o comando **Iniciar**.

A tarefa inicia; o status **Executando** da tarefa será exibido no painel de resultados.

Para visualizar o log de tarefas,

no painel de resultados do node **Verificação de Áreas Críticas**, clique no link **Abrir log de tarefas**.

Alteração do conjunto de componentes e reparação do Kaspersky Embedded Systems Security for Windows

Os componentes do Kaspersky Embedded Systems Security for Windows 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 ao gerenciamento do aplicativo for protegido por senha, o Kaspersky Embedded Systems Security for Windows vai solicitá-la quando você tentar remover ou modificar o conjunto de componentes no Assistente de instalação.

Para modificar o conjunto de componentes do Kaspersky Embedded Systems Security for Windows:

1. No menu **Iniciar**, selecione **Todos os programas** > **Kaspersky Embedded Systems Security for Windows** > **Modificar ou remover o Kaspersky Embedded Systems Security for Windows**.

   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 for Windows ou 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 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. No menu de contexto selecione **O componente não estará disponível**.

Clique no botão **Avançar**.

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

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

Caso ocorram problemas na operação do Kaspersky Embedded Systems Security for Windows (travamentos do Kaspersky Embedded Systems Security for Windows; tarefas que travam ou não iniciam), é possível executar um reparo do Kaspersky Embedded Systems Security for Windows. Você pode executar um reparo salvando as configurações atuais do Kaspersky Embedded Systems Security for Windows ou pode selecionar uma opção para reinicializar todas as configurações do Kaspersky Embedded Systems Security for Windows com os seus valores padrão.

Para reparar o Kaspersky Embedded Systems Security for Windows após o travamento do aplicativo ou de uma tarefa:

1. No menu **Iniciar**, selecione **Todos os programas**.
2. Selecione **Kaspersky Embedded Systems Security for Windows**.
3. Selecione **Modificar ou remover o Kaspersky Embedded Systems Security for Windows**.

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

   Isso abre a janela **Reparar componentes instalados**.
5. Na janela **Reparar componentes instalados**, marque a caixa de seleção **Restaurar configurações recomendadas do aplicativo** se desejar redefinir as configurações do aplicativo e restaurar o Kaspersky Embedded Systems Security for Windows com suas configurações padrão. Clique no botão **Avançar**.
6. Na janela **Pronto para reparar**, confirme a operação de reparo clicando no botão **Instalar**.
7. Na janela exibida quando a operação de reparação for concluída, clique no botão **OK**.

O Kaspersky Embedded Systems Security for Windows será reparado com base nas configurações especificadas.

Desinstalação usando o Assistente de instalação

Esta seção contém instruções sobre a remoção do Kaspersky Embedded Systems Security for Windows e do Console do Aplicativo de um dispositivo protegido usando o Assistente de instalação/desinstalação.

Desinstalação do Kaspersky Embedded Systems Security for Windows

Os arquivos de despejo e rastreamento não são excluídos na desinstalação do Kaspersky Embedded Systems Security for Windows. Você pode excluir manualmente os arquivos de despejo e rastreamento da pasta especificada durante a configuração da gravação dos arquivos de despejo e rastreamento.

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

O Kaspersky Embedded Systems Security for Windows pode ser desinstalado do dispositivo protegido usando o Assistente de instalação/Desinstalação.

Uma reinicialização pode ser necessária após a desinstalação do Kaspersky Embedded Systems Security for Windows de um dispositivo protegido. A reinicialização pode ser adiada.

A desinstalação, reparação 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 ao gerenciamento do aplicativo for protegido por senha, o Kaspersky Embedded Systems Security for Windows vai solicitá-la quando você tentar remover ou modificar o conjunto de componentes no Assistente de instalação.

Para desinstalar o Kaspersky Embedded Systems Security for Windows:

1. No menu **Iniciar**, selecione **Todos os programas**.
2. Selecione **Kaspersky Embedded Systems Security for Windows**.
3. Selecione **Modificar ou remover o Kaspersky Embedded Systems Security for Windows**.

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

   A janela **Configurações avançadas de desinstalação do aplicativo** é exibida.
5. 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 for Windows exporte objetos que foram colocados em quarentena. Por padrão, a caixa de seleção fica desmarcada.

   b. Marque a caixa de seleção **Exportar objetos do backup** para exportá-los a partir do Backup do Kaspersky Embedded Systems Security for Windows. Por padrão, a caixa de seleção fica desmarcada.

   c. Clique no botão **Salvar em** e selecione a pasta para onde deseja exportar os objetos. Por padrão, os objetos serão exportados para %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall.

   Clique no botão **Avançar**.

6. Na janela **Pronto para desinstalar**, confirme a desinstalação clicando no botão **Desinstalar**.

7. Na janela exibida quando a desinstalação for concluída, clique no botão **OK**.

O Kaspersky Embedded Systems Security for Windows será desinstalado do dispositivo protegido.

Desinstalação do Console do Kaspersky Embedded Systems Security for Windows

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

Você pode desinstalar o Console do Aplicativo do dispositivo protegido usando o Assistente de instalação/desinstalação.

Após desinstalar o Console do Aplicativo, não será necessário reiniciar o dispositivo protegido.

Para desinstalar o Console do Aplicativo:

1. No menu **Iniciar**, selecione **Todos os programas**.

2. Selecione **Kaspersky Embedded Systems Security for Windows**.

3. Selecione **Modificar ou remover o Kaspersky Embedded Systems Security for Windows**.
   A janela **Reparar ou remover a instalação** do assistente é exibida.

4. Selecione **Remover componentes do software** e clique no botão **Avançar**.

5. A janela **Pronto para desinstalar** é exibida. Clique no botão **Desinstalar**.
   A janela **Desinstalação concluída** é exibida.

6. Clique no botão **OK**.

A desinstalação estará concluída e o Assistente de instalação será 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 for Windows na linha de comando e contém exemplos de comandos para instalar e desinstalar o Kaspersky Embedded Systems Security for Windows na linha de comando e exemplos de comandos para adicionar e remover os componentes do Kaspersky Embedded Systems Security for Windows na linha de comando.

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

Os arquivos de despejo e rastreamento não são excluídos na desinstalação do Kaspersky Embedded Systems Security for Windows. Você pode excluir manualmente os arquivos de despejo e rastreamento da pasta especificada durante a configuração da gravação dos arquivos de despejo e rastreamento.

É possível instalar ou desinstalar o Kaspersky Embedded Systems Security for Windows e adicionar ou remover seus componentes ao executar o arquivo do pacote de instalação \exec\ess_x86.msi ou \exec\ess_x64.msi a partir da linha de comando após especificar as configurações de instalação usando opções na linha de comando.

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

Execute a instalação usando uma conta incluída no grupo de administradores no dispositivo protegido onde o aplicativo estiver instalado.

Caso um dos arquivos \exec\ess_x86.msi ou\exec\ess_x64.msi seja executado no dispositivo protegido sem opções adicionais na linha de comando, o Kaspersky Embedded Systems Security for Windows será instalado com as configurações de instalação padrão.

É possível atribuir o conjunto de componentes a ser instalado usando a opção de linha de comando ADDLOCAL e listando os códigos dos componentes selecionados ou conjuntos de componentes.

Exemplos de comandos para instalar o Kaspersky Embedded Systems Security for Windows

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

Em dispositivos protegidos executando uma versão de 32 bits do Microsoft Windows, execute os arquivos com o sufixo x86 no kit de distribuição. Em dispositivos protegidos 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 for Windows usando o arquivo setup.exe

Para instalar o Kaspersky Embedded Systems Security for Windows com as configurações de instalação recomendadas sem interação do usuário, execute o seguinte comando:

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

Você pode instalar o Kaspersky Embedded Systems Security for Windows com as seguintes configurações:

- Instale apenas os componentes de Proteção de Arquivos em Tempo Real e de Verificação por Demanda
- Não execute a Proteção de Arquivos em Tempo Real ao iniciar o Kaspersky Embedded Systems Security for Windows

- Não exclua os arquivos recomendados pela Microsoft Corporation do escopo da verificação

Para instalar os componentes, como o Controle de Dispositivos, execute o seguinte comando:

```
\exec\setup.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0 /p ADDMSEXCLUSION=0
```

Ao instalar o Kaspersky Embedded Systems Security for Windows em computadores com dispositivos de rede e dispositivos SCSI que causam uma falha no sistema após a instalação de aplicativo, as seguintes opções adicionais podem ser usadas com este comando:

`/p SKIP_NETWORK_UPPERFILTERS=<1|0>`

Ativa (1) ou desativa (0) a interceptação de conexões de adaptadores de rede.

`/p SKIP_SCSIADAPTER_UPPERFILTERS=<2|0>`

Ativa (1) ou desativa (0) a interceptação de conexões de adaptadores SCSI.

Lista de comandos usados para a instalação: executar um arquivo .msi

Para instalar o Kaspersky Embedded Systems Security for Windows com as configurações de instalação recomendadas sem interação do usuário, execute o seguinte comando:

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

Para instalar o Kaspersky Embedded Systems Security for Windows com as configurações de instalação recomendadas e visualizar a interface da instalação, execute o seguinte comando:

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

Para instalar o Kaspersky Embedded Systems Security for Windows com as configurações de instalação recomendadas e ativar a rotação de arquivos de rastreamento quando o número de arquivos de rastreamento atingir o número máximo especificado, execute o seguinte comando:

```
msiexec /i ess.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1
PRIVACYPOLICY=1
```

O parâmetro `TRACE_FOLDER` é necessário.

As seguintes regras se aplicam ao parâmetro `TRACE_MAX_ROLL_COUNT`:

- Caso esse parâmetro seja especificado, a rotação do arquivo de rastreamento será ativada quando o número de arquivos de rastreamento atingir o número máximo especificado no parâmetro. Intervalo de valores de parâmetros disponível: de 1 a 999.

- Caso o número máximo de arquivos de rastreamento seja especificado como 0, a rotação de arquivos de rastreamento será desativada.

- Caso um valor de parâmetro seja especificado, mas seja inválido ou esteja fora do intervalo de valores disponível (de 1 a 999), a rotação de arquivos de rastreamento será ativada com o número máximo padrão de arquivos de rastreamento definido como 5.

- Caso o parâmetro não seja especificado:

  - Caso a rotação de arquivos de rastreamento já esteja configurada no dispositivo, as configurações não serão alteradas. O aplicativo ignorará os parâmetros inseridos.

  - Caso a rotação de arquivos de rastreamento não esteja configurada no dispositivo, a opção de rotação será ativada com o número máximo padrão de arquivos de rastreamento definido como 5.

Para instalar e ativar o Kaspersky Embedded Systems Security for Windows 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 for Windows 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 for Windows na pasta de instalação C:\ESS, execute o seguinte comando:

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

Para instalar o Kaspersky Embedded Systems Security for Windows e salvar um arquivo de log de instalação com o nome ess.log na pasta onde o arquivo msi do Kaspersky Embedded Systems Security for Windows está armazenado, 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 for Windows, execute o seguinte comando:

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

Para instalar e ativar o Kaspersky Embedded Systems Security for Windows usando o arquivo de chave C:\0000000A.key e configurar o Kaspersky Embedded Systems Security for Windows de acordo com as configurações descritas no arquivo de configuração C:\settings.xml, 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 for Windows estiver protegido por senha, execute o seguinte comando:

```
msiexec /p "<nome do arquivo msp com caminho>" UNLOCK_PASSWORD=<senha>
```

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security for Windows

O Kaspersky Embedded Systems Security for Windows iniciará as tarefas de proteção e verificação imediatamente após a instalação se o aplicativo tiver sido ativado. Se você selecionar a opção **Ativar a proteção de arquivos em tempo real após a instalação do aplicativo (recomendado)** durante a instalação do Kaspersky Embedded Systems Security for Windows, o aplicativo verificará os objetos do sistema de arquivos do dispositivo quando forem acessados. O Kaspersky Embedded Systems Security for Windows 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 for Windows:

- Inicie a tarefa de atualização do banco de dados do Kaspersky Embedded Systems Security for Windows. Após a instalação, o Kaspersky Embedded Systems Security for Windows verificará objetos usando o banco de dados incluído no respectivo kit de distribuição. Recomendamos atualizar imediatamente o banco de dados do Kaspersky Embedded Systems Security for Windows. 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, é possível iniciar a tarefa atualização do banco de dados do aplicativo executando o seguinte comando:

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

Neste caso, as atualizações dos bancos de dados do Kaspersky Embedded Systems Security for Windows são baixadas dos servidores de atualização da Kaspersky. A conexão com a fonte de atualização é estabelecida por meio do servidor proxy (endereço do servidor proxy: proxy.company.com, porta: 8080) utilizando 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 dispositivo se nenhum software antivírus com proteção de arquivos em tempo real estiver instalado no dispositivo antes da instalação do Kaspersky Embedded Systems Security for Windows.

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 de administrador sobre eventos do Kaspersky Embedded Systems Security for Windows.

Adicionar/remover componentes. Exemplos de comandos

O componente de Controle de Inicialização de Aplicativos é instalado automaticamente.

Para instalar o componente de Verificação por Demanda, execute o seguinte comando:

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

ou

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

Depois de adicionar os componentes na lista, o Kaspersky Embedded Systems Security for Windows reinstala os componentes existentes e instala os componentes especificados.

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

```
msiexec /i ess.msi REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

Para instalar novos componentes, execute o seguinte comando:

```
msiexec /i ess.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas
EULA=1 PRIVACYPOLICY=1 /qn
```

Depois de listar os componentes que deseja instalar e remover, o Kaspersky Embedded Systems Security for Windows instala e remove os componentes correspondentes.

Desinstalação do Kaspersky Embedded Systems Security for Windows. Exemplos de comandos

Para desinstalar o Kaspersky Embedded Systems Security for Windows do dispositivo protegido, execute o seguinte comando:

- Para sistemas operacionais de 32 bits:
  `msiexec /x ess_x86.msi /qn`
- Para sistemas operacionais de 64 bits:
  `msiexec /x ess_x64.msi /qn`

ou

- Para sistemas operacionais de 32 bits:
  `msiexec /x {263DB314-C453-4539-A5C1-845B542FFDCA} /qn`
- Para sistemas operacionais de 64 bits:
  `msiexec /x {429EF48A-879D-428A-BA60-22761417FD8E} /qn`

Para desinstalar o Console do Kaspersky Embedded Systems Security for Windows, execute o seguinte comando:

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

ou

```
msiexec /x {4A79347C-BAE9-4A94-BF5D-16CDA5085084} /qn
```

Para desinstalar o Kaspersky Embedded Systems Security for Windows de um dispositivo em que a proteção de senha esteja ativa, execute o comando a seguir:

- Para sistemas operacionais de 32 bits:
  `msiexec /x {263DB314-C453-4539-A5C1-845B542FFDCA} UNLOCK_PASSWORD=*** /qn`
- Para sistemas operacionais de 64 bits:
  `msiexec /x {429EF48A-879D-428A-BA60-22761417FD8E} UNLOCK_PASSWORD=*** /qn`

Códigos de retorno

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

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 for Windows. Para instalar o aplicativo, inicie o assistente de instalação com direitos de administrador local.
25003	O Kaspersky Embedded Systems Security for Windows não pode ser instalado em dispositivos 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 os seguintes softwares: <lista de softwares incompatíveis>.
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 sobre a instalação do Kaspersky Embedded Systems Security for Windows usando o Kaspersky Security Center, uma descrição do procedimento de instalação e desinstalação do Kaspersky Embedded Systems Security for Windows pelo Kaspersky Security Center e uma descrição das ações a serem executadas após o Kaspersky Embedded Systems Security for Windows ter sido instalado.

Informações gerais sobre a instalação por meio do Kaspersky Security Center

Você pode instalar o Kaspersky Embedded Systems Security for Windows através do Kaspersky Security Center usando a tarefa de instalação remota.

Após a conclusão da tarefa de instalação remota, o Kaspersky Embedded Systems Security for Windows será instalado com configurações idênticas em vários dispositivos protegidos.

Todos os dispositivos protegidos podem ser combinados em um único grupo de administração e uma tarefa de grupo pode ser criada para instalar o Kaspersky Embedded Systems Security for Windows nos dispositivos protegidos desse grupo.

Você pode criar uma tarefa para instalar remotamente o Kaspersky Embedded Systems Security for Windows em um conjunto de dispositivos protegidos que não estejam no mesmo grupo de administração. Ao criar essa tarefa você deve gerar uma lista dos dispositivos protegidos individuais nos quais o Kaspersky Embedded Systems Security for Windows 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 for Windows

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

- Se o Agente de rede do Kaspersky Security Center já estiver instalado em dispositivos protegidos onde o Kaspersky Embedded Systems Security for Windows será instalado (independentemente do domínio onde os dispositivos protegidos estão localizados ou se eles pertencem a algum domínio).

  Caso o agente de rede ainda não esteja instalado nos dispositivos protegidos, é possível instalá-lo com o Kaspersky Embedded Systems Security for Windows utilizando uma tarefa de instalação remota. Antes de instalar o Agente de Rede, certifique-se de que a conta que deseja especificar na tarefa esteja incluída no grupo de administradores de cada um dos dispositivos protegidos.

- Todos os dispositivos protegidos nos quais deseja instalar o Kaspersky Embedded Systems Security for Windows estão no mesmo domínio do Servidor de Administração, e o Servidor de Administração está registrado como a conta do **Administrador do Domínio** (caso essa conta tenha direitos de administrador local nos dispositivos protegidos do domínio).

Por padrão, ao usar o método de **Instalação forçada**, a tarefa de instalação remota será executada a partir da conta que está executando o Servidor de Administração.

Ao trabalhar com tarefas de grupo ou com tarefas para conjuntos de dispositivos protegidos no modo de instalação (desinstalação) forçada, uma conta deve ter os seguintes direitos dispositivo protegido:

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

Instalação do Kaspersky Embedded Systems Security for Windows através 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 for Windows através do Kaspersky Security Center no futuro, certifique-se de que as seguintes condições sejam cumpridas:

- O dispositivo protegido no qual o Servidor de Administração do Kaspersky Security Center está instalado também tem o Plug-in de Administração instalado (arquivo \exec\klcfginst.exe no kit de distribuição do Kaspersky Embedded Systems Security for Windows).
- O Agente de Rede do Kaspersky Security Center está instalado nos dispositivos protegidos. Se o Agente de rede do Kaspersky Security Center não estiver instalado nos dispositivos protegidos, você poderá instalá-lo junto com o Kaspersky Embedded Systems Security for Windows usando uma tarefa de instalação remota.

Os dispositivos também podem ser combinados em um grupo de administração 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 for Windows usando uma tarefa de instalação remota:

1. Inicialize do Console de Administração do Kaspersky Security Center.
2. No Kaspersky Security Center, expanda o node **Avançado**.
3. Expanda o node secundário **Instalação remota**.
4. No painel de resultados do node secundário **Pacotes de instalação**, clique no botão **Criar um pacote de instalação**.
5. Selecione o tipo de pacote de instalação **Criar pacote de instalação para um aplicativo da Kaspersky**.
6. Insira o nome do novo pacote de instalação.
7. Especifique o arquivo ess.kud do kit de distribuição do Kaspersky Embedded Systems Security for Windows como o arquivo do pacote de instalação.

   A janela **Contrato de Licença do Usuário Final e Política de Privacidade** é exibida.
8. Caso concorde com os termos e condições do Contrato de Licença do Usuário Final e da Política de Privacidade, marque as caixas de seleção **Confirmo que li completamente, entendi e aceito os termos e condições deste Contrato de Licença do Usuário Final** e marque as caixas de seleção **Estou ciente e concordo que meus dados serão manuseados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade. Confirmo que li completamente e entendi a Política de Privacidade** para prosseguir com a instalação.

   Você deve aceitar o Contrato de Licença e a Política de Privacidade para prosseguir.
9. Para alterar o conjunto de componentes a serem instalados do Kaspersky Embedded Systems Security for Windows e as configurações de instalação padrão no pacote de instalação:
   a. No Kaspersky Security Center, expanda o node **Instalação remota**.
   b. No painel de resultados do node secundário **Pacotes de instalação**, abra o menu de contexto do pacote de instalação do Kaspersky Embedded Systems Security for Windows criado e selecione **Propriedades**.
   c. Na janela **Propriedades: <nome do pacote de instalação>**, abra a seção **Configurações**.

      No grupo de configurações **Componentes a ser instalados**, marque as caixas de seleção junto dos nomes dos componentes do Kaspersky Embedded Systems Security for Windows que você deseja instalar.
   d. 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 dispositivo protegido, ela será criada.
   e. No grupo **Configurações avançadas de instalação**, defina as seguintes configurações:
      - **Verificar a existência de vírus no dispositivo protegido antes da instalação**
      - **Ativar a proteção em tempo real após a instalação do aplicativo**
      - **Adicionar arquivos recomendados pela Microsoft à lista de exclusões**

- **Adicionar arquivos recomendados pela Kaspersky à lista de exclusões**
- **Ativar inicialização atrasada do Kaspersky Security Service juntamente com a inicialização do sistema operacional**

f. Na janela de diálogo **Propriedades: <nome do pacote de instalação>**, clique em **OK**.

10. No node **Pacotes de instalação**, crie uma tarefa para instalar remotamente o Kaspersky Embedded Systems Security for Windows nos dispositivos protegidos 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*.

11. Execute a tarefa de instalação remota do Kaspersky Embedded Systems Security for Windows.

O Kaspersky Embedded Systems Security for Windows será instalado nos dispositivos protegidos especificados na tarefa.

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security for Windows

Após instalar o Kaspersky Embedded Systems Security for Windows, recomendamos que você atualize os bancos de dados do Kaspersky Embedded Systems Security for Windows nos dispositivos e execute uma Verificação de áreas críticas dos dispositivos caso nenhum aplicativo de antivírus com a função de Proteção em tempo real ativada estivesse instalado nos dispositivos antes da instalação do Kaspersky Embedded Systems Security for Windows.

Se os dispositivos protegidos nos quais o Kaspersky Embedded Systems Security for Windows foi instalado fizerem parte de um único grupo de administração no Kaspersky Security Center, é possível executar essas tarefas usando os seguintes métodos:

1. Criar tarefas de atualização do banco de dados para o grupo de dispositivos protegidos nos quais o Kaspersky Embedded Systems Security for Windows foi instalado. Defina o Servidor de Administração do Kaspersky Security Center como a fonte de atualização.

2. Crie uma tarefa de grupo de Verificação por Demanda com o status de Verificação de Áreas Críticas. O Kaspersky Security Center avalia o status de segurança de cada dispositivo protegido no grupo com base nos resultados dessa tarefa, não com base nos resultados da tarefa de Verificação de Áreas Críticas.

3. Criar uma nova política para o grupo de dispositivos protegidos. Nas propriedades da política, na seção **Configurações do aplicativo**, desative o início programado das tarefas de Verificação por Demanda do sistema e das tarefas de Atualização do banco de dados nos dispositivos protegidos do grupo de administração nas configurações da subseção **Executar as tarefas do sistema local**.

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

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 node **Avançado**.
2. Expanda o node secundário **Instalação remota**.
3. No painel de resultados do node secundário Pacotes de instalação, clique no botão **Criar um pacote de instalação**. Ao criar o novo pacote de instalação:
   a. Na janela **Assistente de Novo pacote**, selecione **Criar** pacote de instalação para o arquivo executável especificado como o tipo do pacote.
   b. Insira o nome do novo pacote de instalação.
   c. Selecione o arquivo console\setup.exe na pasta do kit de distribuição do Kaspersky Embedded Systems Security for Windows e marque a caixa de seleção **Copiar toda a pasta no pacote de instalação**.
   d. Use a opção de linha de comando ADDLOCAL no campo **Configurações de inicialização de arquivo executável (opcional)** para executar a instalação do Console do Aplicativo. O Console do Aplicativo é instalado na pasta de instalação padrão. Tenha certeza de especificar o parâmetro "EULA=1". Caso contrário, é impossível instalar componentes.
      ```
      /s /p "ADDLOCAL=MmcSnapin EULA=1"
      ```
      Caso seja necessário, no campo **Parâmetros de inicialização de arquivo executável (opcional)**, é possível especificar a opção de linha de comando ADDLOCAL para modificar o conjunto de componentes a ser instalado, e a opção de linha de comando INSTALLDIR para especificar uma pasta de destino diferente da padrão. Por exemplo, para executar uma instalação autônoma do Console do Aplicativo na pasta C:\KasperskyConsole, use a seguinte opção de linha de comando:
      ```
      /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
      ```
4. No nó filho **Pacotes de instalação**, crie uma tarefa para instalar remotamente o Console do Aplicativo nos dispositivos protegidos 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.

5. Execute a tarefa de instalação remota.

O Console do Aplicativo será instalado nos dispositivos protegidos especificados na tarefa.

Desinstalação do Kaspersky Embedded Systems Security for Windows através do Kaspersky Security Center

Os arquivos de despejo e rastreamento não são excluídos na desinstalação do Kaspersky Embedded Systems Security for Windows. Você pode excluir manualmente os arquivos de despejo e rastreamento da pasta especificada durante a configuração da gravação dos arquivos de despejo e rastreamento.

Se o acesso ao gerenciamento do Kaspersky Embedded Systems Security for Windows em dispositivos da rede for protegido por senha, insira a senha ao criar uma tarefa de desinstalação de vários aplicativos. Se a proteção de senha não for gerenciada centralmente por uma política do Kaspersky Security Center, o Kaspersky Embedded Systems Security for Windows será desinstalado dos dispositivos nos quais a senha inserida corresponder ao valor definido. O Kaspersky Embedded Systems Security for Windows não será desinstalado de outros dispositivos protegidos.

Para desinstalar o Kaspersky Embedded Systems Security for Windows:

1. No Console de Administração do Kaspersky Security Center, crie e inicie uma tarefa de remoção do aplicativo.

2. Na tarefa, selecione o método de desinstalação (similar à seleção do método de instalação; consulte a seção anterior) e especifique a conta que o Servidor de Administração usará para acessar os dispositivos protegidos. Você pode desinstalar o Kaspersky Embedded Systems Security for Windows somente com as configurações de desinstalação padrão.

Instalação e desinstalação via políticas de grupo do Active Directory

Esta seção descreve como instalar e desinstalar o Kaspersky Embedded Systems Security for Windows pelas políticas de grupo do Active Directory, assim como descreve as informações sobre as ações que devem ser executadas após a instalação do Kaspersky Embedded Systems Security for Windows pelas políticas de grupo.

Instalação do Kaspersky Embedded Systems Security for Windows através das políticas de grupo do Active Directory

Você pode instalar o Kaspersky Embedded Systems Security for Windows em vários dispositivos protegidos através da política de grupo do Active Directory. Você pode instalar o Console do Aplicativo do mesmo modo.

Os dispositivos protegidos nos quais você deseja instalar o Kaspersky Embedded Systems Security for Windows ou o Console do Aplicativo devem estar em um único domínio e em uma única unidade organizacional.

Os sistemas operacionais nos dispositivos protegidos nos quais você deseja instalar o Kaspersky Embedded Systems Security for Windows por meio da política devem ter os mesmos bits (32 ou 64 bits).

Você deve ter direitos de administrador do domínio.

Para instalar o Kaspersky Embedded Systems Security for Windows, use o pacote de instalação ess_x86.msi ou ess_x64.msi. Para instalar o Console do Aplicativo, use o pacote 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 for Windows (ou o Console do Aplicativo):

1. Salve o arquivo msi do pacote de instalação correspondente à arquitetura (32 ou 64 bits) da versão instalada do sistema operacional Microsoft Windows na pasta compartilhada do controlador do domínio.

2. Salve o arquivo de chave na mesma pasta pública no controlador de domínio.

3. Na mesma pasta compartilhada no controlador de domínio, crie um arquivo install_props.json que contenha as linhas abaixo. Isso significa que você concorda com os termos do Contrato de Licença de Usuário Final e da Política de Privacidade.

```
{
"EULA": "1",
"PRIVACYPOLICY": "1"
}
```

4. No controlador do domínio, crie uma nova política para o grupo ao qual os dispositivos protegidos pertencem.

5. Usando o **Editor de Objetos de Política de Grupo**, crie um novo pacote de instalação no node **Configuração do Computador**. Especifique o caminho para o arquivo msi do Kaspersky Embedded Systems Security for Windows (ou do Console do Aplicativo) no formato UNC (Universal Naming Convention).

6. Marque a caixa de seleção do Windows Installer **Instalar sempre com privilégios elevados** tanto no node **Configuração do Computador** quanto no node **Configuração do Usuário** do grupo selecionado.

7. Aplique as alterações com o comando `gpupdate / force`.

O Kaspersky Embedded Systems Security for Windows será instalado nos dispositivos protegidos do grupo depois que tiverem sido reiniciados.

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security for Windows

Após instalar o Kaspersky Embedded Systems Security for Windows nos dispositivos protegidos, é recomendado atualizar imediatamente os bancos de dados do aplicativo e executar uma verificação nas áreas críticas. Você pode executar essas ações no Console do Aplicativo.

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

Desinstalação do Kaspersky Embedded Systems Security for Windows através das políticas de grupo do Active Directory

Os arquivos de despejo e rastreamento não são excluídos na desinstalação do Kaspersky Embedded Systems Security for Windows. Você pode excluir manualmente os arquivos de despejo e rastreamento da pasta especificada durante a configuração da gravação dos arquivos de despejo e rastreamento.

Se você instalou o Kaspersky Embedded Systems Security for Windows (ou o Console do Aplicativo) no grupo de dispositivos protegidos usando uma política de grupo do Active Directory, poderá usar essa política para desinstalar o Kaspersky Embedded Systems Security for Windows (ou o Console do Aplicativo).

Você só pode desinstalar o aplicativo 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 gerenciamento do aplicativo for protegido por senha, você não poderá desinstalar o Kaspersky Embedded Systems Security for Windows usando as políticas de grupo do Active Directory.

Para desinstalar o Kaspersky Embedded Systems Security for Windows (ou o Console do Aplicativo):

1. No controlador do domínio, selecione a unidade organizacional a qual pertencem os dispositivos protegidos dos quais deseja desinstalar o Kaspersky Embedded Systems Security for Windows ou o Console do Aplicativo.
2. Selecione a política criada para a instalação do Kaspersky Embedded Systems Security for Windows e no **Editor de Objeto de Políticas de Grupo**, no node **Instalação do software** (**Configuração do Computador** >**Configuração do software** > **Instalação do software**), abra o menu de contexto do pacote de instalação do Kaspersky Embedded Systems Security for Windows (ou do Console do Aplicativo) e selecione o comando **Todas as tarefas** > **Remover**.
3. Selecione o método de desinstalação **Desinstalar o software de usuários e computadores imediatamente**.
4. Aplique as alterações com o comando `gpupdate /force`.

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

Verificação das funções do Kaspersky Embedded Systems Security for Windows. Uso do vírus de teste EICAR

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

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 objeto malicioso e não contém um código executável para o seu dispositivo, mas os aplicativos antivírus da maioria dos fornecedores o identificam como uma ameaça.

O arquivo que contém esse vírus de teste chama-se eicar.com. É possível baixá-lo a partir do site do EICAR.

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

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

É possível usar o arquivo eicar.com para verificar como o Kaspersky Embedded Systems Security for Windows desinfecta objetos infectados e como ele detecta objetos possivelmente infectados. Para isso, abra o arquivo usando um editor de texto, adicione um dos prefixos listados na tabela abaixo do 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 for Windows processe o arquivo eicar.com com um prefixo, na seção de configurações de segurança de **Proteção de objetos** defina o valor **Todos os objetos** para as tarefas de Proteção do Computador em Tempo Real e de Verificação por Demanda padrão do Kaspersky Embedded Systems Security for Windows.

Prefixos em arquivos EICAR

Prefixo	Status do arquivo após a verificação e a ação do Kaspersky Embedded Systems Security for Windows
Nenhum prefixo	**O Kaspersky Embedded Systems Security for Windows atribui o status Infectado ao objeto e o exclui.**
SUSP–	O Kaspersky Embedded Systems Security for Windows atribui o status **Possivelmente infectado** ao objeto detectado pelo analisador heurístico e o exclui já que objetos possivelmente infectados não são desinfetados.
WARN–	O Kaspersky Embedded Systems Security for Windows atribui o status **Possivelmente infectado** ao objeto (o código do objeto corresponde em parte ao código de uma ameaça conhecida) e o exclui, já que objetos possivelmente infectados não são desinfectados.
CURE–	O Kaspersky Embedded Systems Security for Windows 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".

Verificação dos recursos de Proteção de Arquivos em Tempo Real e Verificação por Demanda

Após instalar o Kaspersky Embedded Systems Security for Windows, é possível confirmar se o Kaspersky Embedded Systems Security for Windows detecta objetos contendo códigos maliciosos. Para isso, use o vírus de teste EICAR.

Para verificar o recurso de Proteção de Arquivos em Tempo Real:

1. Baixe o arquivo eicar.com a partir do site do EICAR. Salve-o em uma pasta compartilhada na unidade local de qualquer dispositivo 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 desejar verificar o funcionamento das notificações de usuário de rede, certifique-se de que o serviço Windows Messenger da Microsoft esteja ativado tanto no dispositivo protegido quanto no dispositivo onde você salvou o arquivo eicar.com.

3. Abra o Console do Aplicativo no dispositivo protegido.

4. Copie o arquivo eicar.com salvo para a unidade local do dispositivo protegido usando um dos seguintes métodos:

   - Para testar as notificações por meio da janela de Serviços de Terminal, copie o arquivo eicar.com para o dispositivo protegido após conectar-se a ele usando o utilitário Remote Desktop Connection.

   - Para testar notificações por meio do serviço Windows Messenger da Microsoft, use os locais da rede do dispositivo para copiar o arquivo eicar.com do dispositivo onde você o salvou.

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

- O arquivo eicar.com será excluído do dispositivo protegido.
- No Console do Aplicativo, o log de tarefas recebe o status de *Crítico*. O log tem uma nova linha com informações sobre uma ameaça no arquivo eicar.com.
- A seguinte mensagem do serviço Windows Messenger da Microsoft aparece no dispositivo de onde o arquivo foi copiado: `O Kaspersky Embedded Systems Security for Windows bloqueou o acesso ao <caminho do arquivo no dispositivo >\eicar.com no computador <nome do dispositivo na rede> às <hora em que o evento ocorreu>. Razão: Ameaça detectada. Vírus: EICAR-Test-File. Nome de usuário: <nome de usuário>. Nome do computador: <nome da rede do dispositivo a partir da qual o arquivo foi copiado>.`

  Certifique-se de que o serviço Windows Messenger da Microsoft esteja funcionando no dispositivo do qual você copiou o arquivo eicar.com.

Para verificar o recurso de Verificação por Demanda:

1. Baixe o arquivo eicar.com a partir do site do EICAR. Salve-o em uma pasta compartilhada na unidade local de qualquer dispositivo 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 e expanda o node **Verificação por demanda** na árvore do Console do Aplicativo.
3. Selecione o node secundário **Verificação de Áreas Críticas**.
4. Na guia **Configurações do escopo da verificação**, abra o menu de contexto no node **Rede** e selecione **Adicionar arquivo de rede**.
5. Insira o caminho de rede para o arquivo eicar.com no dispositivo remoto no formato UNC (Universal Naming Convention).
6. Marque a caixa de seleção **Caminho para o objeto** para incluir o caminho de rede adicionado ao escopo da verificação.
7. Executar a tarefa de Verificação de áreas críticas.

A Verificação por Demanda estará funcionando corretamente se as seguintes condições forem atendidas:

- O arquivo eicar.com será excluído da unidade de disco rígido do dispositivo.
- No Console do Aplicativo, o log de tarefas recebe o status de *Crítico*. O log de tarefas Verificação de áreas críticas tem uma nova linha com as informações sobre uma ameaça no arquivo eicar.com.

Interface do aplicativo

É possível controlar o Kaspersky Embedded Systems Security for Windows utilizando as seguintes interfaces:

- Console do Aplicativo local.
- Console de administração do Kaspersky Security Center.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Console de Administração do Kaspersky Security Center

O Kaspersky Security Center permite instalar e desinstalar, iniciar e interromper o Kaspersky Embedded Systems Security for Windows, definir as configurações do aplicativo, alterar o conjunto de componentes disponíveis do aplicativo, adicionar chaves e iniciar e interromper tarefas remotamente.

O aplicativo pode ser gerenciado por meio do Kaspersky Security Center utilizando o Plug-in de Administração do Kaspersky Embedded Systems Security for Windows. Consulte as informações detalhadas sobre a interface do Kaspersky Security Center na *Ajuda do Kaspersky Security Center*.

Kaspersky Security Center Web Console e Cloud Console

O Kaspersky Security Center Web Console (doravante também denominado Web Console) é um aplicativo destinado a executar centralmente as principais tarefas de gerenciamento e manutenção do sistema de segurança da rede de uma organização. O Web Console é um componente do Kaspersky Security Center que fornece uma interface de usuário. Para obter informações detalhadas sobre o Kaspersky Security Center Web Console, consulte a *Ajuda do Kaspersky Security Center*.

O Kaspersky Security Center Cloud Console (doravante também denominado Cloud Console) é uma solução baseada em nuvem para proteger e gerenciar a rede de uma organização. Para obter informações detalhadas sobre o Kaspersky Security Center Cloud Console, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

O Web Console e o Cloud Console permitem fazer o seguinte:

- Monitorar o status do sistema de segurança da organização.
- Instalar os aplicativos da Kaspersky nos dispositivos da rede.
- Gerenciar aplicativos instalados.
- Visualizar os relatórios sobre o status do sistema de segurança.

Licenciamento do aplicativo

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

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.

É possível ler os termos do Contrato de Licença do Usuário Final e da Política de Privacidade que descrevem o processamento e a transmissão de dados, das seguintes maneiras:

- Durante a instalação do Kaspersky Embedded Systems Security for Windows.
- No menu **Iniciar** (**Todos os programas** > **Kaspersky Embedded Systems Security for Windows** > **EULA e Política de Privacidade**) após a instalação.
- Durante a instalação do Kaspersky Fraud Prevention Cloud.
- Lendo o documento do arquivo license.txt incluído no kit de distribuição.
- No site da Kaspersky (https://www.kaspersky.ru/business/eula).

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 utilização do aplicativo, concedido ao usuário sob o Contrato de Licença do Usuário Final.

Uma licença válida permite que você receba o uso do aplicativo de acordo com os termos do Contrato de Licença do Usuário Final, bem como receba suporte técnico quando necessário.

O escopo do serviço e o período do uso do aplicativo dependem do tipo de licença usada para ativar o aplicativo.

É possível ativar o aplicativo de duas maneiras:

- Usando um arquivo de chave, que concede o uso sob uma licença comercial
- Usando um código de ativação para comprar uma licença comercial.

É possível comprar a licença padrão do Kaspersky Embedded Systems Security for Windows ou a licença estendida do Kaspersky Embedded Systems Security for Windows Compliance Edition, que inclui dois componentes adicionais de inspeção do sistema: Monitor de Integridade do Sistema e Inspeção do Log.

Quando uma licença comercial expira, o aplicativo continua em execução, mas alguns dos seguintes recursos ficam indisponíveis:

- Integração com a Kaspersky Security Network
- Atualização do banco de dados do Kaspersky Embedded Systems Security for Windows.

Caso a chave de licença seja removida, o aplicativo continuará sendo executado. Caso uma licença seja removida, o aplicativo continuará em execução; as tarefas de **Verificação por demanda** e **Proteção de arquivos em tempo real** permanecem disponíveis, porém todas as outras tarefas e as atualizações do banco de dados do Kaspersky Embedded Systems Security for Windows estarão indisponíveis. O mesmo acontece se a Kaspersky adicionar sua licença na lista de permissões.

Para continuar utilizando todos os recursos do Kaspersky Embedded Systems Security for Windows, é necessário renovar a licença.

Para garantir a proteção máxima do dispositivo, é recomendado renovar a licença antes que ela expire.

Certifique-se de que a data de validade da chave adicional é posterior à da chave ativa

Sobre o certificado da licença

Um *certificado de licença* é um documento fornecido junto com um arquivo de chave ou código de ativação (se for o caso).

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

- 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 validade da licença ou termo da licença
- Tipo de licença

Sobre a chave

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

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 pode adicionar uma chave à lista de bloqueio devido a 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 ou de avaliação pode ser adicionada como a 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 o arquivo de chave

Um *arquivo de chave* é um arquivo com a extensão .key fornecido pela Kaspersky. Os arquivos de chave são concebidos para adicionar uma chave que ativa o aplicativo.

O usuário recebe um arquivo de chave por e-mail depois de comprar o Kaspersky Embedded Systems Security for Windows ou depois de solicitar a versão de avaliação do Kaspersky Embedded Systems Security for Windows.

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

Você pode restaurar um arquivo de chave se ele for acidentalmente excluído. Um arquivo de chave para o registro com a Kaspersky CompanyAccount poderá ser necessário.

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

- Entrar em contato com o fornecedor da licença.
- Obter um arquivo de chave no site da Kaspersky de acordo com o código de ativação disponível.

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 for Windows. Você recebe um código de ativação no endereço de e-mail fornecido ao comprar o Kaspersky Embedded Systems Security for Windows ou ao encomendar a versão de avaliação do Kaspersky Embedded Systems Security for Windows.

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

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 o código de ativação, entre em contato com o parceiro da Kaspersky Lab de quem a licença foi comprada.

Sobre a coleta de dados

O Contrato de Licença do Kaspersky Embedded Systems Security for Windows, 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 recebidos pela Kaspersky durante a utilização do aplicativo são protegidos e processados conforme a Política de Privacidade disponível em www.kaspersky.com/Products-and-Services-Privacy-Policy.

Os termos do Contrato de Licença e da Política de Privacidade estão disponíveis durante a instalação do Kaspersky Embedded Systems Security for Windows, como parte do kit de distribuição e no menu **Iniciar** (**Todos os programas** > **Kaspersky Embedded Systems Security for Windows** > **EULA e Política de Privacidade**) após a instalação.

Durante a desinstalação do Kaspersky Embedded Systems Security for Windows, todos os dados armazenados por ele no dispositivo protegido serão excluídos.

Ao aceitar os termos do Contrato de Licença de Usuário Final, você aceita enviar automaticamente os seguintes dados para a Kaspersky:

- 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.

- Para usar a capacidade de navegar pelos artigos da Base de Conhecimento quando ocorrerem erros no aplicativo (serviço Redirecionador) – informações sobre o aplicativo e tipo de link: o nome, a localidade e o número da versão completa do aplicativo, o tipo de link de redirecionamento 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 os 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.

Processamento local de dados

Enquanto as funções principais do aplicativo descritas neste Manual são executadas, o Kaspersky Embedded Systems Security for Windows processa e armazena localmente uma sequência de dados no dispositivo protegido.

A tabela abaixo contém informações sobre o processamento e o armazenamento local dos dados contidos nos relatórios no Kaspersky Embedded Systems Security for Windows.

Processamento e armazenamento de dados contidos nos relatórios

Área funcional	Registro de eventos
Tipo de uso	O Kaspersky Embedded Systems Security for Windows armazena os dados localmente e os envia ao Servidor de Administração. O banco de dados do Servidor de Administração armazena informações sobre os eventos de aplicativos que ocorrem nos dispositivos protegidos gerenciados.
Armazenamento	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<versão do produto>\Reports

	• %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • Banco de dados do Servidor de Administração
Medidas de segurança	Lista de controle de acesso.
Período de armazenamento	Os dados são armazenados até a desinstalação do Kaspersky Embedded Systems Security for Windows. Durante a desinstalação do Kaspersky Embedded Systems Security for Windows, todos os dados armazenados por ele no dispositivo protegido serão excluídos.
Finalidade	Fornecimento do recurso primário.

O Kaspersky Embedded Systems Security for Windows não exclui eventos no Log de Eventos do Windows, inclusive os eventos que ocorrem durante sua desinstalação.

Para fornecer o recurso de registro de eventos, o Kaspersky Embedded Systems Security for Windows processa localmente os seguintes dados:

- Nomes, somas de verificação (MD5, SHA-256) e atributos de arquivos processados e seus caminhos completos na mídia verificada.
- Ações executadas em arquivos verificados pelo Kaspersky Embedded Systems Security for Windows.
- Ações do usuário executadas em arquivos verificados no dispositivo protegido.
- Informações sobre contas de usuários que executam ações na rede ou no dispositivo protegido.
- Valores do Caminho da instância do dispositivo para dispositivos adicionados às regras de Controle de Dispositivos.
- Informações sobre processos e scripts em execução no sistema: somas de verificação (MD5, SHA-256), caminhos completos para arquivos executáveis e informações sobre certificados digitais.
- Configurações do Firewall do Windows.
- Entradas do Log de Eventos do Windows.
- Nomes de contas de usuário que executam ações em arquivos verificados no dispositivo protegido.
- Instâncias de arquivos executáveis que estão sendo inicializados e os tipos, nomes, somas de verificação e atributos desses arquivos.
- Informações sobre a atividade da rede:
  - Os endereços IP dos dispositivos externos bloqueados.
  - Endereços IP processados.
- Informações sobre o status do USN Journal do Windows.

A tabela a seguir contém informações sobre os dados de serviço processados pelo Kaspersky Embedded Systems Security for Windows. Os dados do serviço incluem: parâmetros do programa, arquivos em quarentena e de backup, informações nos bancos de dados de serviço do programa e dados da licença.

A tabela abaixo contém informações sobre o processamento e o armazenamento local de dados relacionados aos parâmetros especificados por um usuário no Kaspersky Embedded Systems Security for Windows.

Processamento e armazenamento de dados relacionados aos parâmetros especificados por um usuário

Área funcional	Todos os recursos do Kaspersky Embedded Systems Security for Windows
Tipo de uso	O Kaspersky Embedded Systems Security for Windows armazena os dados localmente e os envia ao Servidor de Administração. Os dados são armazenados no banco de dados do Servidor de Administração. Os dados processados localmente pelo aplicativo não são enviados automaticamente à Kaspersky ou a outros sistemas de terceiros.
Armazenamento	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\ <versão do produto>\ • Banco de dados do Servidor de Administração
Medidas de segurança	Lista de controle de acesso.
Período de processamento	Os dados são armazenados até a desinstalação do Kaspersky Embedded Systems Security for Windows. Durante a desinstalação do Kaspersky Embedded Systems Security for Windows, todos os dados armazenados por ele no dispositivo protegido serão excluídos. O Kaspersky Embedded Systems Security for Windows não exclui os dados relacionados aos parâmetros exportados para o arquivo de configuração. O Kaspersky Embedded Systems Security for Windows não exclui objetos em Quarentena e de Backup se as caixas de seleção **Exportar objetos da quarentena** e **Exportar objetos do backup** estiverem marcadas no Assistente de instalação.
Finalidade	Fornecimento do recurso primário.

Para fins específicos, o Kaspersky Embedded Systems Security for Windows processa localmente os seguintes dados:

- Objetos colocados em Quarentena ou Backup.
- Informações sobre contas de usuário (nomes de usuário e senhas) nas quais o Kaspersky Embedded Systems Security for Windows executa tarefas.
- Senha do Kaspersky Embedded Systems Security for Windows.
- Endereços IP e identificadores de sessões de logon bloqueadas.
- Configurações do Firewall do Windows e das regras do Firewall do Windows.
- Soma de verificação (MD5, SHA-256) e caminhos para arquivos executáveis adicionados às regras da tarefa de Controle de Inicialização de Aplicativos.
- Valores do Caminho da instância do dispositivo para dispositivos adicionados às regras de Controle de Dispositivos.
- Informações sobre arquivos e pastas incluídos nos escopos das tarefas do Kaspersky Embedded Systems Security for Windows.
- Endereços IP incluídos ou excluídos do escopo da proteção.

- Informações sobre os eventos no Log de Eventos do Windows.
- Informações sobre as detecções com o uso da tecnologia iSwift ou iChecker.
- Soma de verificação (MD5, SHA-256), caminhos completos e máscaras especificados nas configurações de exclusões.
- Informações sobre os processos adicionados à Zona Confiável.
- Informações sobre as chaves de licença adicionadas.
- Informações sobre os certificados digitais.
- Arquivos descompactados de um arquivo ou outro objeto composto durante a verificação.

O Kaspersky Embedded Systems Security for Windows processa e armazena dados como parte da funcionalidade básica do aplicativo, inclusive para registrar em log os 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 for Windows permite configurar o nível de proteção dos dados processados localmente (Gerenciamento das permissões de acesso para as funções do Kaspersky Embedded Systems Security for Windows, Registro de eventos. Logs do Kaspersky Embedded Systems Security for Windows). É possível alterar os privilégios do usuário para acessar dados processados, alterar os períodos de retenção desses dados, desativar inteira ou parcialmente a funcionalidade que envolve o registro em log de dados e alterar o caminho e os atributos da pasta nas quais os dados são registrados.

Os dados processados localmente pelo aplicativo não são enviados automaticamente à Kaspersky ou a outros sistemas de terceiros.

Por padrão, todos os dados processados localmente pelo aplicativo durante a operação são removidos após a desinstalação do Kaspersky Embedded Systems Security for Windows do dispositivo protegido.

Arquivos com informações de diagnóstico (arquivos de rastreamento e despejo), eventos do aplicativo no Log de Eventos do Windows e arquivos com configurações exportadas do Kaspersky Embedded Systems Security for Windows são uma exceção. Recomendamos excluir esses arquivos manualmente.

Você pode encontrar as informações detalhadas sobre o trabalho com arquivos que contêm dados de diagnóstico do aplicativo nas seções correspondentes deste Guia.

É possível excluir os arquivos de Log de Eventos do Windows que contenham eventos do aplicativo Kaspersky Embedded Systems Security for Windows usando ferramentas padrão do sistema operacional.

Processamento local de dados por meio dos componentes auxiliares do aplicativo

O pacote de instalação do Kaspersky Embedded Systems Security for Windows contém os componentes auxiliares do aplicativo, que podem ser instalados no dispositivo mesmo se o Kaspersky Embedded Systems Security for Windows não estiver instalado nele. Esses componentes auxiliares são:

- O Console do Aplicativo. Esse componente está incluído como parte das Ferramentas de Administração do Kaspersky Embedded Systems Security for Windows, sendo um snap-in do Console de Gerenciamento da Microsoft.
- O Plug-in de Administração. Este componente fornece uma integração completa com o aplicativo do Kaspersky Security Center.

Ao executar as funções principais do aplicativo descrito neste Guia, os componentes auxiliares do aplicativo processam e armazenam localmente um conjunto de dados sobre o dispositivo protegido onde estão instalados, mesmo se forem instalados separadamente do Kaspersky Embedded Systems Security for Windows.

Os componentes do aplicativo processam e armazenam localmente os seguintes dados:

- O Console do Aplicativo: o nome do dispositivo protegido com o Kaspersky Embedded Systems Security for Windows instalado (endereço IP ou nome do domínio) ao qual o Console do Aplicativo se conectou remotamente por último; parâmetros de exibição configurados no snap-in do Console de Gerenciamento da Microsoft; dados sobre a última pasta na qual o usuário selecionou objetos pelo Console do Aplicativo (usando a caixa de diálogo do sistema aberta ao clicar no botão **Procurar**). Os arquivos de rastreamento do Console do Aplicativo também podem conter os seguintes dados: o nome do dispositivo protegido com o Kaspersky Embedded Systems Security for Windows instalado com o qual a conexão remota foi estabelecida e o nome da conta de usuário na qual a conexão remota foi estabelecida.

- O Plug-in de Administração pode processar e armazenar temporariamente dados processados pelo Kaspersky Embedded Systems Security for Windows; por exemplo, definições configuradas das tarefas e componentes do aplicativo, configurações das políticas do Kaspersky Security Center e dados enviados em listas de rede.

A tabela abaixo contém informações sobre o processamento e o armazenamento local dos dados gravados em arquivos de despejo e rastreio no Kaspersky Embedded Systems Security for Windows.

O Kaspersky Embedded Systems Security for Windows processa e armazena localmente os seguintes dados gravados em arquivos de despejo e rastreamento:

- Informações sobre as ações executadas pelo Kaspersky Embedded Systems Security for Windows no dispositivo protegido.

- Informações sobre os objetos processados pelo Kaspersky Embedded Systems Security for Windows.

- Informações sobre a atividade no dispositivo protegido processadas pelo Kaspersky Embedded Systems Security for Windows.

- Informações sobre erros que ocorreram durante a execução do Kaspersky Embedded Systems Security for Windows.

Os dados processados pelos componentes auxiliares não são automaticamente enviados à Kaspersky ou outros sistemas de terceiros.

Por padrão, todos os dados processados localmente pelos componentes auxiliares do aplicativo durante a operação são excluídos após a remoção desses componentes.

A exceção são os arquivos de rastreamento de componentes auxiliares do aplicativo. Recomendamos excluir esses arquivos manualmente.

Dados em arquivos de rastreamento e despejo

O Kaspersky Embedded Systems Security for Windows pode, de acordo com as configurações, gravar informações de depuração para rastrear arquivos para fins de suporte técnico durante sua operação.

Os arquivos de despejo do Kaspersky Embedded Systems Security for Windows são gerados pelo sistema operacional durante falhas do aplicativo e são substituídos pela próxima falha.

Os arquivos de rastreamento e despejo podem incluir quaisquer dados pessoais de um usuário ou dados confidenciais da sua organização.

Não use o Kaspersky Embedded Systems Security for Windows em dispositivos para os quais o envio de dados é proibido pela política da sua organização.

Por padrão, o Kaspersky Embedded Systems Security for Windows não registra informações de depuração.

Os arquivos de rastreamento e despejo não são enviados automaticamente para outro host além daquele no qual foram gerados. O conteúdo dos arquivos de rastreamento pode ser exibido usando visualizadores de arquivos de texto padrão. Os arquivos de rastreamento e despejo são mantidos indefinidamente e não são excluídos durante a desinstalação do Kaspersky Embedded Systems Security for Windows.

Informações de depuração podem ser úteis para o Suporte Técnico.

Nenhum mecanismo especial é fornecido para limitar o acesso a arquivos de rastreamento e despejo. O administrador pode configurar esses dados para serem gravados em uma pasta protegida.

Por padrão, o caminho para a pasta do arquivo de rastreamento e despejo não está configurado. Para usar a pasta de rastreamento e despejo, o administrador deve especificá-la.

Os dados nos arquivos de rastreamento e despejo podem conter:

- Informações sobre as ações executadas pelo Kaspersky Embedded Systems Security for Windows no dispositivo protegido.
- Informações sobre objetos processados pelo Kaspersky Endpoint Agent.
- Erros decorrentes durante a operação do Kaspersky Endpoint Agent.

Ativar o aplicativo com um arquivo de chave

Você pode ativar o Kaspersky Embedded Systems Security for Windows aplicando um arquivo de chave.

Se uma chave ativa já tiver sido adicionado ao Kaspersky Embedded Systems Security for Windows e você adicionar outra chave como a chave ativa, a nova chave substitui a chave adicionada anteriormente. A chave adicionada anteriormente é removida.

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

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

Para ativar o Kaspersky Embedded Systems Security for Windows usando um arquivo de chave:

1. Na árvore do Console do Aplicativo, expanda o node **Licenciamento**.
2. No painel de resultados do node **Licenciamento**, clique no link **Adicionar chave**.
3. Na janela que se abre, clique no botão **Procurar**.
4. Selecione um arquivo de chave com a extensão .key.

Você também pode adicionar uma chave como chave adicional. Para adicionar uma chave adicional, marque a caixa de seleção **Usar como chave adicional**.

5. Clique no botão **OK**.

O arquivo de chave selecionado será aplicado. As informações sobre a chave adicionada estarão disponíveis no node **Licenciamento**.

Ativação do aplicativo com um código

Para ativar o aplicativo usando um código de ativação, o dispositivo protegido deve estar conectado à Internet.

Você pode ativar o Kaspersky Embedded Systems Security for Windows usando um código de ativação.

Com esse método, o Kaspersky Embedded Systems Security for Windows envia dados ao servidor de ativação para verificar o código inserido:

- Se a verificação do código de ativação for bem-sucedida, o aplicativo é ativado.
- Se a verificação do código de ativação falhar, a notificação correspondente será exibida. Nesse caso, você deve entrar em contato com o fornecedor de software de quem você comprou a licença do Kaspersky Embedded Systems Security for Windows.
- Se o número de ativações com o código de ativação for excedido, a notificação correspondente será exibida. O procedimento de ativação do aplicativo será interrompido e o aplicativo sugerirá que o usuário entre em contato com o Suporte Técnico da Kaspersky.

É possível ativar o Kaspersky Embedded Systems Security for Windows com um código de ativação utilizando o Console do Aplicativo ou criando a tarefa de grupo de Ativação do aplicativo por meio do Plug-in de Administração ou do plug-in da Web.

Para ativar o Kaspersky Embedded Systems Security for Windows com um código de ativação utilizando o Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o node **Licenciamento**.
2. No painel de resultados do node **Licenciamento**, clique no link **Adicionar código de ativação**.
3. Na janela exibida, insira o código de ativação no campo **Código de ativação**.
   - Se desejar usar o código de ativação como uma chave adicional, ative a caixa de seleção **Usar como chave adicional**.
   - Para exibir informações sobre uma licença, clique no botão **Exibir as informações da licença**. As informações serão exibidas no bloco **Informações da licença**.
4. Clique no botão **OK**.

   O Kaspersky Embedded Systems Security for Windows envia informações sobre o código de ativação aplicado para o servidor de ativação.

Visualização das informações sobre a licença atual

Visualizando informações de licenciamento

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

- **Verificando o status principal** – o Kaspersky Embedded Systems Security for Windows está verificando o arquivo de chave ou o código de ativação aplicado e aguardando uma resposta sobre o status atual da chave.
- **Data de expiração da licença** – o Kaspersky Embedded Systems Security for Windows 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 foi aplicada.
  - A chave adicionada foi colocada na lista de bloqueio e está prestes a ser bloqueada.
- **A licença expirou** – o Kaspersky Embedded Systems Security for Windows 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 for Windows não está ativado porque os termos do Contrato de Licença do Usuário Final foram violados. O status é realçado em vermelho.
- **A chave está na lista de bloqueio** – a chave adicionada foi bloqueada e colocada na lista de bloqueio pela Kaspersky, por exemplo, caso a chave tenha sido utilizada por terceiros para ativar o aplicativo ilegalmente. O status é realçado em vermelho.

Visualização das informações sobre a licença atual

Para visualizar informações sobre a licença atual,

na árvore do Console do Aplicativo, expanda o node **Licenciamento**.

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

Informações gerais sobre a licença no node Licenciamento

Campo	Descrição
Código de ativação	O 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. A coluna **Status da ativação** do painel de detalhes do node de **Licenciamento** pode ter os seguintes status: • **Aplicada** - se você ativou o aplicativo usando um código de ativação ou arquivo de chave. • **Ativação** - se você aplicou um código de ativação para ativar o aplicativo, mas o processo de ativação ainda não foi finalizado. O status muda para **Aplicada** quando a ativação do aplicativo é concluída e o conteúdo do painel de detalhes do node é atualizado.

	• **Erro de ativação** - se a ativação do aplicativo falhou. Você pode visualizar a causa da ativação mal sucedida no log de tarefas.
Chave	A chave usada para ativar o aplicativo.
Tipo de licença	Tipo de licença: comercial ou de avaliação.
Data de expiração	Data e hora de expiração da licença associada a uma chave ativa.
Status do código de ativação ou da chave	Status do código de ativação ou da chave: *Ativa* ou *Adicional*.

Para visualizar informações detalhadas sobre a licença,

no node de **Licenciamento**, abra o menu de contexto na linha com os dados da licença que deseja expandir e selecione **Propriedades**.

Na janela **Propriedades 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 ou do revendedor de quem o Kaspersky Embedded Systems Security for Windows foi adquirido (consulte a tabela abaixo).

Informações detalhadas da licença na janela Propriedades: <Status de Código de ativação ou status da chave>

Campo	Descrição
Guia Geral	
Chave	A chave usada 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 ou de avaliação.
Dias até a expiração	Número de dias restantes até a expiração da licença associada à chave ativa.
Data de expiração	Data e hora de expiração da licença associada a uma chave ativa. Caso o aplicativo seja ativado com uma assinatura ilimitada, o valor do campo é *Ilimitado*. Caso o Kaspersky Embedded Systems Security for Windows não seja capaz de determinar a data de expiração da licença, o valor do campo é definido como *Desconhecido*.
Aplicativo	O nome do aplicativo ativado com o arquivo de chave ou código de ativação.
Restrição de uso da chave	Restrição de uso da chave (se houver).
Elegível para suporte técnico	Informações sobre se a Kaspersky ou um de seus parceiros fornecerá Suporte técnico de acordo com os termos da licença.
Guia Avançado	
Informações sobre a licença	Chave da licença atual.
Informações	Detalhes de contato da Kaspersky ou de seu parceiro que fornece suporte técnico. Este

de suporte	campo pode ficar vazio se o suporte técnico não for fornecido.
Informações do proprietário	Informações sobre o proprietário da licença: o nome do cliente e o nome da organização para a qual a licença foi adquirida.

Limitações funcionais quando a licença expira

Quando a licença atual expira, as seguintes limitações são aplicadas aos componentes funcionais:

- Todas as tarefas serão interrompidas, exceto as tarefas de Proteção de Arquivos em Tempo Real, Verificação sob Demanda e Controle de Integridade de Aplicativos.
- Não é possível iniciar nenhuma tarefa, exceto a Proteção de Arquivos em Tempo Real, Verificação sob Demanda e Controle de Integridade de Aplicativos. 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 (repositórios, logs, informações de diagnóstico) ainda estarão disponíveis.

Renovação da licença

Por padrão, o Kaspersky Embedded Systems Security for Windows notifica o usuário quando restam 14 dias para a licença expirar. Nesse caso, o status **Data de expiração da licença** é realçado em amarelo no painel de resultados do node **Kaspersky Embedded Systems Security for Windows**.

Você pode renovar a licença antes da data de expiração usando um arquivo de chave adicional. Isto garante que seu dispositivo permaneça protegido após a expiração da licença atual e antes que você ative o aplicativo com uma nova licença.

Para renovar uma licença:

1. Obtenha um novo código de ativação ou um arquivo de chave.
2. Na árvore do Console do Aplicativo, selecione o node **Licenciamento**.
3. Execute uma das seguintes ações no painel de resultados do node **Licenciamento**:
   - Se deseja renovar uma licença usando um arquivo de chave:
     a. Clique no link **Adicionar chave**.
     b. Na janela que se abre, clique no botão **Procurar**.
     c. Selecione um novo arquivo de chave com a extensão .key.
     d. 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 no botão **OK**.

A chave adicional serão adicionados e automaticamente aplicados após a expiração da licença atual do Kaspersky Embedded Systems Security for Windows.

Exclusão da chave

Você pode remover a chave adicionada.

Se uma chave adicional tiver sido adicionada ao Kaspersky Embedded Systems Security for Windows 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 node **Licenciamento**.
2. No painel de resultados do node **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.

Trabalhar com o Plug-in de Administração

Esta seção fornece informações sobre o Plug-in de Administração do Kaspersky Embedded Systems Security for Windows e descreve como gerenciar o aplicativo instalado em um dispositivo protegido ou em um grupo de dispositivos protegidos.

Gerenciamento do Kaspersky Embedded Systems Security for Windows a partir do Kaspersky Security Center

É possível gerenciar de forma centralizada vários dispositivos protegidos, que tenham o Kaspersky Embedded Systems Security for Windows instalado e que façam parte do mesmo grupo de administração, por meio do Plug-in de Administração do Kaspersky Embedded Systems Security for Windows. O Kaspersky Security Center também permite definir separadamente as configurações de cada dispositivo protegido incluído no grupo de administração.

Um grupo de administração é criado manualmente por meio do Kaspersky Security Center. O grupo inclui vários dispositivos com o Kaspersky Embedded Systems Security for Windows instalado para os quais se 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*.

Não será possível configurar o aplicativo para um único dispositivo protegido caso a operação do Kaspersky Embedded Systems Security for Windows no dispositivo protegido seja controlada por uma política ativa do Kaspersky Security Center.

O Kaspersky Embedded Systems Security for Windows pode ser gerenciado 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 dispositivos. 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 dispositivo protegido>** do Kaspersky Security Center.

  As políticas podem ser usadas para definir configurações gerais do aplicativo, configurações para tarefas de proteção do computador em tempo real, tarefas de controle de atividade em dispositivos e configurações para iniciar as tarefas locais do sistema em um agendamento.

- **Usando tarefas de grupo do Kaspersky Security Center**. Com as tarefas de grupo do Kaspersky Security Center, é possível definir remotamente configurações comuns de tarefas com um período de validade para um grupo de dispositivos.

  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 do Gerador de Regras de Controle de Inicialização de Aplicativos.

- **Usando tarefas para um grupo de dispositivos**. As tarefas para um conjunto de dispositivos permitem definir remotamente as configurações comuns de tarefa com um período de execução limitado para os dispositivos protegidos que não pertencem a nenhum dos grupos de administração.

- **Usando a janela de propriedades de um único dispositivo**. Na janela **Propriedades: <Nome do dispositivo protegido>**, é possível definir remotamente as configurações de tarefa para um dispositivo individual protegido e incluído em um grupo de administração. É possível definir tanto as configurações gerais do aplicativo como as configurações de todas as tarefas do Kaspersky Embedded Systems Security for Windows caso o dispositivo protegido selecionado não seja controlado por uma política ativa do Kaspersky Security Center.

O Kaspersky Security Center permite definir as configurações do aplicativo, além de trabalhar com logs e notificações. É possível definir essas configurações para um grupo de dispositivos protegidos, assim como para um dispositivo protegido individual.

Gerenciamento das configurações do aplicativo

Esta seção contém informações sobre como definir as configurações gerais do Kaspersky Embedded Systems Security for Windows no Kaspersky Security Center Web Console.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das configurações gerais por meio da política

Para abrir as configurações do aplicativo do Kaspersky Embedded Systems Security for Windows a partir da política:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Configurações do aplicativo**.
6. Clique no botão **Configurações** na subseção da configuração que deseja definir.

Abertura das configurações gerais na janela de propriedades do aplicativo

Para abrir a janela de propriedades do Kaspersky Embedded Systems Security for Windows de um único dispositivo protegido:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Dispositivos**.
4. Abra a janela **Propriedades: <Nome do dispositivo protegido>** usando uma das seguintes maneiras:
   - Clique duas vezes no nome do dispositivo protegido.

- Abra o menu de contexto do nome do dispositivo protegido e selecione o item **Propriedades**.

A janela **Propriedades: <Nome do dispositivo protegido>** é exibida.

5. Na seção **Aplicativos**, selecione **Kaspersky Embedded Systems Security 3.3 for Windows**.
6. Clique no botão **Propriedades**.
   A janela de Configurações do **Kaspersky Embedded Systems Security 3.3 for Windows** é exibida.
7. Selecione a seção **Configurações do aplicativo**.

Definição das configurações gerais do aplicativo no Kaspersky Security Center

Você pode definir configurações gerais para o Kaspersky Embedded Systems Security for Windows através do Kaspersky Security Center para um grupo de dispositivos protegidos ou para um dispositivo protegido.

Definição das configurações de escalabilidade, interface e verificação no Kaspersky Security Center

Para definir as configurações de escalabilidade, interface e verificação:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Configurações do aplicativo**, na subseção **Configurações de escalabilidade, interface e verificação**, clique no botão **Configurações**.
5. Na janela **Configurações avançadas do aplicativo**, na guia **Geral**, defina as seguintes configurações:
   - Na seção **Configurações de escalabilidade**, defina as configurações que definem o número de processos usados pelo Kaspersky Embedded Systems Security for Windows:
     - Detectar automaticamente as configurações de escalabilidade
     - Definir manualmente o número de processos em andamento
       - Número de processos para a Proteção em Tempo Real
       - Número de processos de tarefas de verificação por demanda em segundo plano

- Na seção **Interação com o usuário**, configure se o ícone da bandeja do sistema será exibido na área de notificação marcando ou desmarcando a caixa **Exibir o ícone da Bandeja do Sistema na barra de tarefas**.

6. Na guia **Configurações de verificação**, defina as seguintes configurações:

   - **Restaurar os atributos do arquivo após a verificação**
   - **Limitar a utilização da CPU para threads de verificação**
     - **Limite superior (porcento)**
   - **Pasta para os arquivos temporários criados durante a verificação**

7. Na guia **Armazenamento hierárquico**, selecione a opção para acessar o armazenamento hierárquico.

8. Clique no botão **OK**.

As configurações de aplicativo definidas são salvas.

Definição das configurações de segurança no Kaspersky Security Center

Para definir as configurações de segurança manualmente:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Configurações do aplicativo**, clique no botão **Segurança e confiabilidade** nas definições de **Configurações**.

5. Na janela **Configurações de segurança**, defina as seguintes configurações:

   - Na seção **Configurações de proteção de senha**, ative ou desative a opção **Proteger os processos de aplicativos contra ameaças externas**.
   - Na seção **Configurações de proteção de senha**, defina uma senha para proteger o acesso às funções do Kaspersky Embedded Systems Security for Windows.
   - Na seção **Autodefesa**, defina as configurações de recuperação de tarefas do Kaspersky Embedded Systems Security for Windows quando o aplicativo retornar um erro ou for encerrado.
     - **Executar recuperação da tarefa**
     - **Configurações de confiabilidade**

- Na seção **Recupere tarefas de verificação por demanda não mais do que (vezes)**, especifique as limitações na carga do dispositivo protegido criadas pelo Kaspersky Embedded Systems Security for Windows após mudar para uma fonte de energia UPS:
  - **Não iniciar tarefas de verificação agendadas**
  - **Interromper tarefas de verificação atuais**
- Na seção **Configurações de proteção de senha**, defina uma senha para proteger o acesso às funções do Kaspersky Embedded Systems Security for Windows.

6. Clique no botão **OK**.

As configurações de escalabilidade e de confiabilidade são salvas.

Definição das configurações de conexão usando o Kaspersky Security Center

As configurações de conexão definidas são usadas para conectar o Kaspersky Embedded Systems Security for Windows 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 node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Configurações do aplicativo**, clique no botão **Conexões** na subseção **Configurações**.

   A janela **Configurações de conexão** é exibida.
5. 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**
     - Usar o servidor proxy especificado
     - **Endereço IP ou nome simbólico do servidor proxy e o número da porta**
     - **Ignorar servidor proxy para endereços locais**.
   - 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. O 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 com um nome de usuário e senha usando o 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 de usuário e a senha, se necessário.

- Na seção **Licenciamento**, desmarque ou marque **Usar o Kaspersky Security Center como servidor proxy ao ativar o aplicativo**.

6. Clique no botão **OK**.

As configurações de conexão definidas são salvas.

Configuração da inicialização programada de tarefas locais do 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 dispositivo protegido 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 dispositivo protegido 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 uma tarefa local do sistema é proibida pela política.

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

Caso não utilize a atualização de grupo ou as tarefas de Verificação por Demanda, permita que as tarefas locais do sistema sejam iniciadas na política. O Kaspersky Embedded Systems Security for Windows executará atualizações do banco de dados do aplicativo e do módulo e iniciará todas as tarefas locais do sistema de verificação por demanda de acordo com a programação padrão.

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

- Tarefas de Verificação por Demanda: Verificação de Áreas Críticas. Verificação da Quarentena, Verificação na Inicialização do Sistema Operacional, Controle de Integridade de Aplicativos, Monitor de Comparação de Integridade de Arquivos.

- Tarefas de Atualização: Atualização do Banco de Dados, Atualização dos Módulos de Software, Copiar Atualizações.

Caso o dispositivo protegido seja excluído do grupo de administração, a programação de tarefas locais do sistema será ativada automaticamente.

Para permitir ou bloquear a inicialização programada de tarefas locais do sistema do Kaspersky Embedded Systems Security for Windows em uma política:

1. No node **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 deseja configurar o início programado de tarefas locais do sistema do Kaspersky Embedded Systems Security for Windows para os dispositivos protegidos do grupo, selecione **Propriedades**.
3. Na janela **Propriedades: <Nome da política>**, abra a seção **Configurações do aplicativo**. Na seção **Executar as tarefas do sistema local**, clique no botão **Configurações** e execute uma das seguintes ações:
   - Marque as caixas de seleção **Tarefas de verificação por demanda** e **Tarefas de atualização e tarefa de cópia de atualização** para permitir a inicialização programada das tarefas listadas.
   - Desmarque as caixas **Tarefas de verificação por demanda** e **Tarefas de atualização e tarefa de cópia de atualização** para desativar a inicialização programada das tarefas listadas.

   Marcar ou desmarcar a caixa de seleção não afetará as configurações de inicialização de quaisquer tarefas locais personalizadas desse tipo.
4. Certifique-se de que a política que sendo configurada esteja ativa e seja aplicada ao grupo de dispositivos protegidos selecionados.
5. Clique no botão **OK**.

As definições da tarefa programada configurada são aplicadas às tarefas selecionadas.

Definição das configurações de Quarentena e de Backup no Kaspersky Security Center

Para definir as configurações gerais do Backup no Kaspersky Security Center:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Suplementar**, clique no botão **Configurações** na subseção **Armazenamentos**.

5. Use a guia **Configurações de armazenamentos** da janela **Backup** para definir as configurações de Backup a seguir:

   - Caso queira especificar a pasta de backup, use o campo **Pasta de backup** para selecionar a pasta requerida na unidade local do dispositivo protegido ou insira o caminho completo.

   - Para configurar o tamanho máximo do Backup, marque a caixa de seleção **Tamanho máximo do backup (MB)** e especifique o valor relevante em megabytes no campo de entrada.

   - Para definir o limite de espaço livre do Backup:

     - Defina a configuração do valor do **Tamanho máximo do backup (MB)**.

     - Marque a caixa de seleção **Valor limite de espaço disponível (MB)**.

     - Especifique o valor mínimo de espaço livre na pasta de Backup em megabytes.

   - Para especificar uma pasta para objetos restaurados, execute uma das seguintes ações:

     - Selecione a pasta relevante em uma unidade local do dispositivo protegido na seção **Configurações de restauração**.

     - Insira o nome da pasta e o caminho completo para ela no campo **Pasta destino para a restauração de objetos**.

6. Na janela **Configurações de armazenamentos** na guia **Quarentena**, defina as seguintes configurações da Quarentena:

   - Para alterar a pasta de Quarentena, no campo de entrada da **Pasta da Quarentena**, especifique o caminho completo da pasta na unidade local do dispositivo 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 entrada.

   - 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 entrada.

   - Para alterar a pasta na qual os objetos são restaurados a partir da Quarentena, no campo **Pasta destino para a restauração de objetos**, especifique o caminho completo para a pasta na unidade local do dispositivo protegido.

7. Clique no botão **OK**.

As configurações de Quarentena e Backup definidas são salvas.

Criação e configuração de políticas

Esta seção fornece informações sobre a utilização de políticas do Kaspersky Security Center para gerenciar o Kaspersky Embedded Systems Security for Windows em vários dispositivos protegidos.

As políticas globais do Kaspersky Security Center podem ser criadas para gerenciar a proteção em vários dispositivos onde o Kaspersky Embedded Systems Security for Windows está instalado.

Uma política impõe as configurações, funções e tarefas do Kaspersky Embedded Systems Security for Windows especificadas nela a todos os dispositivos protegidos para 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 for Windows. Essas informações podem ser visualizadas no Console do Aplicativo, no node **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 for Windows utiliza os valores de configurações para as quais o ícone nas propriedades da política em dispositivos protegidos foi selecionado. Nesse caso, o Kaspersky Embedded Systems Security for Windows não utiliza os valores das configurações em vigor antes da aplicação da política. O Kaspersky Embedded Systems Security for Windows não aplica os valores de configurações de política ativa para os 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 dispositivo protegido na janela **Propriedades: <Nome do dispositivo protegido>**.

As configurações especificadas e enviadas para o dispositivo protegido usando uma política ativa são salvas nas configurações da tarefa local após a política ativa ser desativada.

Caso uma política defina as configurações de uma tarefa de Proteção do Computador em Tempo Real sendo executada, as configurações definidas pela política serão alteradas imediatamente após a política ser aplicada. Se a tarefa não estiver sendo executada, as configurações serão aplicadas quando ela for iniciada.

Criando uma política

Para criar uma política para um grupo de dispositivos protegidos onde o aplicativo está instalado e em execução:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e, em seguida, selecione o grupo de administração que contém os dispositivos protegidos para os quais deseja criar uma política.

2. No painel de detalhes do grupo de administração selecionado, marque a guia **Políticas** e clique no link **Criar uma política** para iniciar o assistente e criar uma política.

   A janela **Assistente para Novas Políticas** é exibida.

3. Na janela **Selecione o aplicativo para o qual deseja criar uma política de grupo**, selecione Kaspersky Embedded Systems Security for Windows 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 uma configuração de política usada em uma versão anterior do aplicativo:

   a. Marque a caixa de seleção **Usar configurações da política de versões anteriores do aplicativo**.

   b. Clique no botão **Procurar**.

   c. Selecione a política que deseja aplicar.

   d. Clique no botão **Avançar**.

6. Na janela **Seleção do tipo de operação**, no bloco **Método de criação da política**, selecione uma das seguintes opções:

   - **Nova**, para criar uma nova política com as configurações padrão.
   - **Importar a política criada com a versão anterior do Kaspersky Embedded Systems Security for Windows** para usar a política importada como modelo.

7. Na janela **Proteção do Computador em Tempo Real**, configure os componentes do aplicativo:

   a. Caso necessário, altere as configurações padrão dos componentes da Proteção do Computador em Tempo Real:

      1. Clique em **Configurações** na subseção do componente.
      2. Na janela exibida, defina as configurações do componente:
      3. Clique no botão **OK**.

   b. Permitir ou bloquear a aplicação das configurações dos componentes da Proteção do Computador em Tempo Real em dispositivos protegidos na rede:

      - Clique no botão para permitir a definição das configurações do componente do aplicativo em dispositivos protegidos na rede e para bloquear a aplicação das configurações do componente do aplicativo definidas na política.
      - Clique no botão para bloquear a definição das configurações do componente do aplicativo em dispositivos protegidos na rede e para permitir a aplicação das configurações do componente do aplicativo definidas na política.

   c. Clique no botão **Avançar**.

8. Selecione um dos seguintes status de política na janela **Criar política de grupo para o aplicativo**:

   - **Política ativa**, caso queira aplicar a política imediatamente após a 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.
   - Marque a caixa de seleção **Abrir propriedades da política imediatamente após serem criadas** para fechar automaticamente o **Assistente para Novas Políticas** e configurar a política recém-criada após clicar no botão **Próximo**.

9. Clique no botão **Concluir**.

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 for Windows.

Após a criação de uma nova política, um conjunto de regras de permissão é criado para impedir que os aplicativos sejam bloqueados e garantir a operação ininterrupta. É possível exibir as estatísticas da tarefa no log de tarefas. Veja abaixo os detalhes e as limitações.

Por padrão, o Kaspersky Embedded Systems Security for Windows cria um conjunto de regras para o tráfego de rede de entrada quando uma nova política é criada:

- Duas regras de permissão para o processo de compartilhamento da área de trabalho do Windows usando o Agente de Rede do Kaspersky Security Center, localizado nas pastas %Arquivos de Programas% e %Arquivos de Programas (x86)%. Estado: ativado. Endereços externos permitidos: todos. Protocolos: TCP e UPD (uma regra por protocolo).
- Duas regras de permissão para a porta local 15000. Estado: ativado. Endereços externos permitidos: todos. Protocolos: TCP e UPD (uma regra por protocolo).

Por padrão, o Kaspersky Embedded Systems Security for Windows cria um conjunto de regras para o tráfego de rede de saída quando uma nova política é criada:

- Duas regras de permissão para o serviço do Kaspersky Embedded Systems Security for Windows, localizado em %Arquivos de Programas% e %Arquivos de Programas (x86)%. Estado: ativado. Endereços externos permitidos: todos. Protocolos: TCP e UPD (uma regra por protocolo).
- Duas regras de permissão para o processo de trabalho do Kaspersky Embedded Systems Security for Windows, localizado nas pastas %Arquivos de programas% e %Arquivos de programas (x86)%. Estado: ativado. Endereços externos permitidos: todos. Protocolos: TCP e UPD (uma regra por protocolo).
- Duas regras de permissão para a porta local 13000. Estado: ativado. Endereços externos permitidos: todos. Protocolos: TCP e UPD (uma regra por protocolo).

Seções de configurações de política do Kaspersky Embedded Systems Security for Windows

Geral

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

- Indicar o status da política.
- Configurar as configurações de herança das políticas principais e secundárias.

Notificação de evento

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

- *Evento crítico*
- *Falha funcional*

- *Aviso*
- *Informação*
  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 eventos registrados.
- Indicar o método de notificação para eventos registrados.

Configurações do aplicativo

Configurações da seção Configurações do aplicativo

Seção	Opções
Configurações de escalabilidade, interface e verificação	Na subseção **Configurações de escalabilidade, interface e verificação**, 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 e confiabilidade	Na subseção **Segurança e confiabilidade**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Definir as configurações de inicialização da tarefa. • Especificar como o aplicativo deve se comportar quando o dispositivo protegido estiver funcionando com a fonte de energia UPS. • Ativar ou desativar a proteção de senha das funções do aplicativo.
Conexões	Na subseção **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 as tarefas do sistema local	Na subseção **Executar as tarefas do sistema local**, é possível utilizar o botão **Configurações** para permitir ou bloquear a inicialização das seguintes tarefas locais do sistema de acordo com uma programação definida nos dispositivos protegidos: • Tarefa de Verificação por Demanda. • Tarefas de Atualização e Cópia de Atualizações.

Suplementar

Configurações da seção Suplementar

Seção	Opções
Zona Confiável	Na subseção **Configurações**, é possível clicar no botão **Zona Confiável** para definir as seguintes configurações da Zona Confiável:

	• 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	Na subseção **Verificação de unidades removíveis**, é possível usar o botão **Configurações** para definir configurações de verificação para drives removíveis.
Permissões de acesso do usuário para gerenciamento do aplicativo	Na subseção **Permissões de acesso do usuário para gerenciamento do aplicativo**, é possível configurar direitos de usuário e de grupos de usuários para gerenciar o Kaspersky Embedded Systems Security for Windows.
Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service	Na subseção **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service**, é possível configurar os direitos de usuário e de grupos de usuários para gerenciar o Kaspersky Security Service.
Armazenamentos	Na seção **Armazenamentos**, clique no botão **Configurações** para definir as seguintes configurações de Quarentena, Backup e Hosts Bloqueados: • Especificar o caminho da pasta onde deseja colocar objetos em Quarentena ou de Backup. • Configurar o tamanho máximo do Backup e Quarentena, alem de especificar o limite de espaço disponível. • Especificar o caminho da pasta onde deseja colocar os objetos restaurados da Quarentena ou Backup. • Configurar a forma como hosts longos são bloqueados.

Proteção do Computador em Tempo Real

Configurações da seção Proteção do Computador em Tempo Real

Seção	Opções
Proteção de Arquivos em Tempo Real	Na subseção **Proteção de Arquivos em Tempo Real**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Indicar o modo de proteção. • Configurar o uso do Analisador Heurístico. • Configurar o aplicativo 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 **Declaração da KSN** para aceitar ou rejeitar a Declaração da KSN e definir as configurações de troca de dados.
Prevenção de Exploits	Na subseção **Prevenção de Exploits**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Selecionar o modo de proteção da memória do processo. • Indicar ações para reduzir os riscos de exploit. • Adicionar e editar a lista de processos protegidos.

Controle de atividades locais

Configurações da seção Controle de Atividades Locais

Seção	Opções
Controle de inicialização de aplicativos	Na subseção **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 das regras de Controle de Inicialização de Aplicativos. • Configurar o uso da KSN. • Definir as configurações de inicialização da tarefa.
Controle de dispositivos	Na subseção **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 atividades de rede

Configurações da seção Controle de Atividades de Rede

Seção	Opções
Gerenciamento de firewall	Na subseção **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

Configurações da seção Inspeção do Sistema

Seção	Opções
Monitor de Integridade de Arquivos	Na subseção **Monitor de Integridade de Arquivos**, é possível configurar o controle sobre alterações em arquivos que podem significar uma violação de segurança em um dispositivo protegido.
Inspeção do Log	Na subseção **Inspeção do Log**, é possível configurar o monitoramento da integridade do dispositivo protegido de acordo com os resultados de uma análise do Log de Eventos do Windows.

Logs e notificações

Configurações da seção Logs e Notificações

Seção	Opções
Logs de tarefas	Na subseção **Logs 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 do Log de tarefas. • Especificar a integração SIEM com configurações do Kaspersky Security Center.
Notificações de evento	Na subseção **Notificações de evento**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Especificar as configurações de notificação de usuário para os eventos *Objeto detectado*, *Dispositivo externo não confiável detectado e restrito* e *Sessão de rede listada como não confiável*. • 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 (incluindo objetos da Quarentena e do Backup) que o Kaspersky Embedded Systems Security for Windows relatará ao Servidor de Administração.

Diagnóstico de falhas

Configurações da seção de diagnóstico de mau funcionamento

Seção	Opções
Configurações de diagnóstico de falhas	Na subseção **Configurações de soluções de problemas**, é possível definir as seguintes opções:

	• Selecione a opção para **Ativar o rastreamento**. • Defina a **Pasta para arquivos de rastreamento**. • Especifique o **Nível de detalhes**. • Defina o **Tamanho máximo dos arquivos de rastreamento**. • Selecione a opção **Remover os arquivos de rastreamento mais antigos**. • Defina o **Número máximo de arquivos para um log de rastreamento**. As configurações da política de grupo e as configurações locais introduzem parâmetros correspondentes. Para saber mais informações sobre as opções e suas limitações, consulte a definição das configurações locais. É possível definir valores diferentes para os parâmetros no dispositivo local e na política de grupo para vários dispositivos com as seguintes condições aplicadas: • As configurações da política de grupo definidas no servidor do Kaspersky Security Center são de maior prioridade sobre as configurações locais. • As configurações da política de grupo definidas no dispositivo local são de menor prioridade sobre as configurações locais.
Configurações do arquivo de despejo	Na subseção **Configurações do arquivo de despejo**, é possível configurar as seguintes opções conforme o caso: • Selecione a opção **Criar o arquivo de despejo**. • Defina a **Pasta de arquivos de despejo**. As configurações da política de grupo e as configurações locais introduzem parâmetros correspondentes. Para saber mais informações sobre as opções e suas limitações, consulte a definição das configurações locais. É possível definir valores diferentes para os parâmetros no dispositivo local e na política de grupo para vários dispositivos com as seguintes condições aplicadas: • As configurações da política de grupo definidas no servidor do Kaspersky Security Center são de maior prioridade sobre as configurações locais. • As configurações da política de grupo definidas no dispositivo local são de menor prioridade sobre as configurações locais.

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.

Configuração de políticas

Para definir as configurações de política:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados**.

2. Expanda o grupo de administração para o qual deseja definir as configurações de política associadas e abra a guia **Políticas** no painel de detalhes.

3. Clique no nome da política que você quer configurar.

4. Abra a janela **Propriedades: <Nome da política>** usando uma das seguintes maneiras:

   - Selecionando a opção **Propriedades** no menu de contexto da política.
   - Clicando no link **Configurar política** no painel de detalhes à direita da política selecionada.
   - Clicando duas vezes na política selecionada.

5. 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 dispositivos protegidos dentro do grupo de administração selecionado.
   - **Política inativa**, se desejar que a política seja aplicada posteriormente a todos os dispositivos protegidos dentro do grupo de administração selecionado.

   A configuração **Política de usuário ausente** não está disponível ao gerenciar o Kaspersky Embedded Systems Security for Windows.

6. Reconfigure o aplicativo em outras seções da política.

   É possível ativar ou desativar a execução de qualquer tarefa em todos os dispositivos protegidos dentro do grupo de administração por meio de uma política do Kaspersky Security Center.

   É possível configurar a aplicação de configurações de política em todos os dispositivos protegidos de rede para cada componente de software individual.

7. Clique no botão **OK**.

As configurações definidas são aplicadas na política.

Criando e configurando uma tarefa usando o Kaspersky Security Center

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

Sobre a criação de tarefa no Kaspersky Security Center

É possível criar tarefas de grupo para grupos de administração e conjuntos de dispositivos protegidos. É possível criar os seguintes tipos de tarefas por meio do Kaspersky Security Center:

- 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
- Monitor de Comparação de Integridade de Arquivos
- 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 dispositivo protegido: na janela **Propriedades <Nome do dispositivo protegido>** na seção **Tarefas**.
- Para um grupo de administração: no painel de detalhes do node do grupo de dispositivos protegidos selecionado na guia **Tarefas**.
- Para um conjunto de dispositivos protegidos: no painel de detalhes do node **Seleções de dispositivos**.

Você pode usar as políticas para desativar as programações de tarefas locais do sistema para Atualização e Verificação por Demanda em todos os dispositivos 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

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 servidor protegido pertence.
     b. No painel de resultados da guia **Dispositivos**, abra o menu de contexto do dispositivo protegido e selecione **Propriedades**.
     c. Na janela exibida, clique no botão **Adicionar** na seção **Tarefas**.
   - Para criar uma tarefa de grupo:
     a. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

b. Selecione o grupo de administração para o qual você deseja criar uma tarefa.

c. No painel de resultados, abra a guia **Tarefas** e selecione **Criar uma tarefa**.

- Para criar uma tarefa para um conjunto personalizado de dispositivos protegidos:

  a. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

  b. Selecione o grupo de administração que contém os dispositivos protegidos.

  c. Selecione um dispositivo protegido ou um conjunto personalizado de dispositivos protegidos.

  d. Na lista suspensa **Executar ação**, selecione a opção **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 3.3 for Windows**, selecione o tipo da tarefa a ser criada.

3. Caso tenha selecionado qualquer tipo de tarefa, exceto Reversão da Atualização do Banco de Dados, Controle de Integridade de Aplicativos ou Ativação do Aplicativo, a janela **Configurações** será exibida. Dependendo do tipo de tarefa, as configurações podem variar:

   - Crie uma tarefa de Verificação por Demanda.
   - Para criar uma tarefa de atualização, defina as configurações da tarefa de acordo com suas necessidades:

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

     b. Clique no botão **Configurações de conexão**. Na janela **Configurações de conexão**, defina as configurações de acesso ao servidor proxy ao se conectar na fonte de atualização.

   - Para criar uma tarefa de Atualização dos Módulos de Software, defina as configurações necessárias de atualização dos módulos do aplicativo na janela **Configurações**:

     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** for selecionado: um reinício do dispositivo protegido poderá ser necessário para aplicar os módulos de software instalados. Se desejar que o Kaspersky Embedded Systems Security for Windows reinicie o dispositivo protegido automaticamente após a conclusão da tarefa, selecione a caixa **Permitir reinício do sistema operacional**.

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

     A Kaspersky não publica pacotes de atualizações planejados nos servidores de atualização para instalação automática; eles podem ser baixados manualmente no site da Kaspersky. Pode ser configurada uma notificação do administrador sobre o evento **Nova atualização agendada 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 da cópia de atualizações**.

- Para criar a tarefa de Ativação do Aplicativo:

  a. Na janela **Configurações de ativação**, especifique o arquivo de chave que deseja usar para ativar o aplicativo.

  b. Marque a caixa de seleção **Usar como chave adicional** se desejar criar uma tarefa para renovar a licença.

- Crie a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos.
- Crie a tarefa do Gerador de Regras de Controle de Dispositivos.

4. Configure a programação da tarefa.

   É possível configurar a programação para todos os tipos de tarefas, exceto a tarefa de Reversão da Atualização do Banco de Dados.

5. Clique no botão **OK**.

6. Se a tarefa estiver sendo criada para um conjunto de dispositivos protegidos, selecione a rede (ou grupo) de dispositivos protegidos na qual a tarefa será executada.

7. Na janela **Seleção de uma conta para a execução da tarefa**, especifique a conta que deseja usar para executar a tarefa.

8. Na janela **Definir nome da tarefa**, insira um nome para a tarefa (com menos de 100 caracteres) sem incluir os símbolos " * < > ? \ | : .

   Recomendamos adicionar o tipo de tarefa ao nome da tarefa (por exemplo, "Verificação por Demanda de pastas compartilhadas").

9. Na janela **Concluir a criação da tarefa**:

   a. Selecione a caixa de seleção **Executar a tarefa após a finalização do Assistente** caso deseje que a tarefa inicie assim que for criada.

   b. Clique no botão **Concluir**.

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

Acesso a configurações da tarefa local e configurações gerais do aplicativo para um computador individual

Caso um aplicativo esteja sob a política do Kaspersky Security Center no momento e caso essa política proíba a alteração das configurações do aplicativo, essas configurações não poderão ser editadas para um computador individual.

Para acessar as configurações da tarefa local de um computador individual:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados**.

2. Selecione o grupo ao qual o dispositivo protegido pertence.

3. No painel de resultados, selecione a guia **Dispositivos**.

4. Abra a janela **Propriedades: <Nome do dispositivo protegido>** usando uma das seguintes maneiras:

   - Clique duas vezes no nome do dispositivo protegido.
   - selecione **Propriedades** no menu de contexto do nome do dispositivo protegido.

   A janela **Propriedades: <Nome do dispositivo protegido>** é exibida.

5. Vá até a seção **Tarefas**.

6. Na lista de tarefas, selecione uma tarefa local para configurar usando uma das seguintes maneiras:

   - clique duas vezes no nome da tarefa
   - selecione uma tarefa na lista e clique no botão **Propriedades**
   - selecione **Propriedades** no menu de contexto do nome da tarefa.

   A janela **Propriedades: <Nome da tarefa>** é exibida.

Para acessar as configurações gerais do aplicativo para um computador individual:

1. Expanda o node **Dispositivos gerenciados** na árvore do Servidor de Administração do Kaspersky Security Center e selecione o grupo ao qual o dispositivo protegido pertence.

2. No painel de resultados, selecione a guia **Dispositivos**.

3. Abra a janela **Propriedades: <Nome do dispositivo protegido>** usando uma das seguintes maneiras:

   - Clique duas vezes no nome do dispositivo protegido.
   - selecione **Propriedades** no menu de contexto do nome do dispositivo protegido.

   A janela **Propriedades: <Nome do dispositivo protegido>** é exibida.

4. Vá até a seção **Aplicativos**.

5. Na lista de aplicativos instalados, selecione Kaspersky Embedded Systems Security for Windows usando uma das seguintes maneiras:

   - clique duas vezes no nome do Kaspersky Embedded Systems Security for Windows
   - selecione Kaspersky Embedded Systems Security for Windows na lista e clique no botão **Propriedades**.
   - selecione o item **Propriedades** no menu de contexto do nome do Kaspersky Embedded Systems Security for Windows.

   A janela **Configurações** do **Kaspersky Embedded Systems Security for Windows** é exibida.

Configurando tarefas de grupo no Kaspersky Security Center

Ao gerenciar o Kaspersky Embedded Systems Security for Windows a partir do Kaspersky Security Center Cloud Console, não é possível adicionar servidores HTTP e FTP personalizados ou pastas de rede manualmente.

Para configurar a tarefa de grupo para múltiplos dispositivos protegidos:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados** e selecione 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.
4. Abra a janela **Propriedades: <Nome da tarefa>** usando 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**.

   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:
     - Na seção **Escopo da verificação**, configure um escopo de verificação.
     - 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:
     - Na seção **Configurações**, defina as configurações de fonte de atualização e otimização de uso de subsistema de disco.
     - Clique no botão **Configurações de conexão** para definir as configurações de conexão da fonte de atualização.
   - Para configurar a tarefa de Atualização dos módulos de software:
     - Acesse a seção **Configurações**.
     - Escolha uma ação a ser executada: copiar e instalar atualizações críticas de módulos de software ou apenas verificar a existência delas.
   - Para configurar a tarefa Copiar atualizações, especifique o conjunto de atualizações e a pasta de destino na seção **Configurações da cópia de atualizações**.
   - Para criar uma tarefa de Ativação do Aplicativo:

- Na seção **Configurações de ativação**, especifique o arquivo de chave que deseja usar para ativar o aplicativo.
- Selecione a caixa **Usar como chave adicional** caso deseje adicionar um código de ativação ou arquivo de chave para renovar a licença.

- Para configurar a geração automática de regras de permissão para Controle de Dispositivos, na seção **Configurações**, especifique as configurações que serão usadas para criar a lista de regras de permissão.

6. Configure a programação da tarefa na seção **Agendamento**. É possível configurar a programação para todos os tipos de tarefas, exceto a tarefa de Reversão da Atualização do Banco de Dados.

7. Na seção **Conta**, especifique a conta cujos direitos serão usados para executar a 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. Clique no botão **OK** na janela **Propriedades: <Nome da tarefa>**.

As recém-definidas configurações da tarefa de grupo são salvas.

As configurações de tarefa de grupo configuráveis estão resumidas na tabela abaixo.

Configurações de tarefas de grupo do Kaspersky Embedded Systems Security for Windows

Tipos de tarefas do Kaspersky Embedded Systems Security for Windows	Seção na janela Propriedades: <Nome da tarefa>	Configurações de tarefa
Gerador de Regras de Controle de Inicialização de Aplicativos	**Configurações**	Ao configurar a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos, é possível selecionar como deseja criar as regras de permissão: • **Criar regras de permissão com base nos aplicativos em execução** • **Criar regras de permissão para aplicativos das pastas**
	Opções	Você pode especificar ações para execução enquanto cria regras de permissão para o controle de inicialização de aplicativos: • **Usar certificado digital** • **Usar assunto e miniatura do certificado digital** • **Se o certificado estiver ausente, usar** • **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 for Windows cria após a conclusão da tarefa.
	Agendamento	É possível definir configurações para a inicialização programada da tarefa.
Gerador de Regras de Controle de Dispositivos	**Configurações**	• Selecione o modo de operação: considere dados de sistema sobre todos os dispositivos externos que já estiveram conectados alguma vez ou considere somente os dispositivos externos conectados atualmente. • Defina as configurações para arquivos de configuração com listas de regras de permissão que o Kaspersky Embedded Systems Security for Windows cria após a conclusão da tarefa.
	Agendamento	É possível definir configurações para a inicialização programada da tarefa.
Ativação do aplicativo	**Configurações de ativação**	Para ativar o aplicativo ou renovar a licença, você pode adicionar um arquivo de chave.
	Agendamento	É possível definir configurações para a inicialização programada da tarefa.
Copiar atualizações	**Fonte de atualização**	É possível especificar o Servidor de Administração do Kaspersky Security Center ou os servidores de atualização da Kaspersky 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. É possível especificar o uso dos servidores de atualização da Kaspersky se servidores personalizados manualmente não estiverem disponíveis.
	Janela **Configurações de conexão**	Na janela **Configurações de conexão**, vinculada à seção **Fonte de atualização**, é possível especificar se a conexão a servidores de atualização da Kaspersky ou a algum outro servidor deve ser estabelecida através do servidor proxy.
	Configurações da cópia de atualizações	Você pode especificar o conjunto de atualizações destinado à cópia. No campo **Pasta para armazenamento local de atualizações copiadas**, especifique o caminho para a pasta que será usada pelo Kaspersky Embedded Systems Security for Windows para armazenar atualizações copiadas.
	Agendamento	É possível definir configurações para a inicialização programada da tarefa.
Atualização do Banco de Dados	**Configurações**	Você pode especificar o Servidor de Administração do Kaspersky Security Center ou servidores de atualização da Kaspersky como a fonte de atualização do aplicativo na caixa de 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. É possível especificar o uso dos servidores de atualização da Kaspersky se servidores personalizados manualmente não estiverem disponíveis.

		Na seção Otimização de uso da 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**	Na janela **Configurações de conexão**, vinculada à seção **Fonte de atualização**, é possível especificar se a conexão a servidores de atualização da Kaspersky ou a algum outro servidor deve ser estabelecida através do servidor proxy.
	Agendamento	É possível definir configurações para a inicialização programada da tarefa.
Atualização dos Módulos de Software	**Fonte de atualização**	É possível especificar o Servidor de Administração do Kaspersky Security Center ou os servidores de atualização da Kaspersky 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. É possível especificar o uso dos servidores de atualização da Kaspersky se servidores personalizados manualmente não estiverem disponíveis.
	Janela **Configurações de conexão**	No grupo **Configurações de conexão da fonte de atualização**, é possível especificar se a conexão a servidores de atualização da Kaspersky ou a algum outro servidor deve ser estabelecida por meio do servidor proxy.
	Configurações	É possível especificar as ações que o Kaspersky Embedded Systems Security for Windows executará caso atualizações críticas do módulo do aplicativo sejam necessárias, assim como após a conclusão da instalação das atualizações críticas. Além disso, é possível especificar se o Kaspersky Embedded Systems Security for Windows receberá informações sobre as atualizações agendadas e disponíveis.
	Agendamento	É possível definir configurações para a inicialização programada da tarefa.
Configurações de Verificação por Demanda	**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**	Na janela **Configurações da verificação por demanda** vinculada da seção **Escopo da verificação**, é possível selecionar um dos níveis de segurança predefinidos ou personalizar o nível de segurança manualmente.
	Opções	No bloco de configurações do **Analisador heurístico**, é possível ativar ou desativar o seu uso para a tarefa de Verificação por Demanda e definir o nível de análise usando um controle deslizante. No grupo **Integração com outros componentes**, é possível 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 tarefa em segundo plano (prioridade baixa) ou considerar a tarefa como uma Verificação de áreas críticas.

	Agendamento	É possível definir configurações para a inicialização programada da tarefa.
Controle de Integridade de Aplicativos	**Agendamento**	É possível definir configurações para a inicialização programada da tarefa.
Monitor de Comparação de Integridade de Arquivos	**Agendamento**	É possível definir configurações para a inicialização programada da tarefa.

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 **Notificação** e **Exclusões do escopo da tarefa**.

Para obter informações detalhadas sobre as definições das configurações nessas seções, consulte a *Ajuda do Kaspersky Security Center*.

Ativação da tarefa de Aplicativo

Para criar uma tarefa de Ativação do Aplicativo:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados** e selecione 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.
4. Abra a janela **Propriedades: <Nome da tarefa>** usando 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**.

   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 de ativação**, especifique o arquivo de chave que deseja usar para ativar o aplicativo. Marque a caixa de seleção **Usar como chave adicional** caso queira adicionar uma chave para renovar a licença.
6. Configure a programação da tarefa na seção **Agendamento** (é possível configurar uma programação 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 executar a 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 as definições das configurações nessas seções, consulte a *Ajuda do Kaspersky Security Center*.

9. Clique no botão **OK** na janela **Propriedades: <Nome da tarefa>**.

   As recém-definidas configurações da tarefa de grupo são salvas.

Tarefas de atualização

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

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados** e selecione 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.
4. Abra a janela **Propriedades: <Nome da tarefa>** usando 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**.

   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 **Fonte de atualização**, faça o seguinte:

   a. Selecione a fonte de atualização:
      - Servidor de Administração do Kaspersky Security Center.
      - Servidores de atualização da Kaspersky.
      - Servidores HTTP ou FTP personalizados ou pastas de rede.

      Para usar uma pasta compartilhada por SMB como uma fonte de atualização, é necessário especificar uma conta de usuário para iniciar uma tarefa.

      É possível especificar o uso dos servidores de atualização da Kaspersky se servidores personalizados manualmente não estiverem disponíveis.

b. Clique no botão **Configurações de conexão**.

c. Na janela **Configurações de conexão** aberta, configure a utilização de um servidor proxy para se conectar aos servidores de atualização da Kaspersky e outros servidores.

d. Para a tarefa de Atualização do banco de dados, na seção **Otimização de uso da E/S de disco**, configure o recurso que reduz a carga de trabalho no subsistema de disco:

> A seção **Otimização de uso da E/S de disco** está disponível apenas para a tarefa de Atualização do banco de dados.

- Diminuir a carga na E/S de disco
- RAM usada para otimização (MB)

6. Para a tarefa de Atualização dos Módulos de Software, na seção **Configurações**, especifique quais ações o Kaspersky Embedded Systems Security for Windows deve executar quando atualizações críticas de módulos de software ou informações sobre as atualizações planejadas estiverem disponíveis.

   Também é possível especificar quais ações o Kaspersky Embedded Systems Security for Windows deve executar quando as atualizações críticas são instaladas.

> A seção **Configurações** está disponível apenas para a tarefa de Atualização dos Módulos de Software.

7. Para a tarefa Copiar atualizações, na seção **Configurações da cópia de atualizações**, especifique o conjunto de atualizações e a pasta de destino.

> A seção **Configurações da cópia de atualizações** está disponível apenas para a tarefa Copiar atualizações.

8. Configure a programação da tarefa na seção **Agendamento** (é possível configurar uma programação 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 executar a tarefa.

> Para obter informações detalhadas sobre as definições das configurações nessas seções, consulte a *Ajuda do Kaspersky Security Center*.

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

As recém-definidas configurações da tarefa de grupo são salvas.

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

Controle de Integridade de Aplicativos

Para configurar a tarefa de grupo de Controle de Integridade de Aplicativos:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados** e selecione 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.
4. Abra a janela **Propriedades: <Nome da tarefa>** usando 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**.

   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 Controle de Integridade de Aplicativos.
6. Configure a programação da tarefa na seção **Agendamento** (é possível configurar uma programação 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 executar a 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 as definições das configurações nessas seções, consulte a *Ajuda do Kaspersky Security Center*.
9. Clique no botão **OK** na janela **Propriedades: <Nome da tarefa>**.

   As recém-definidas configurações da tarefa de grupo são salvas.

Definir configurações de diagnóstico de travamento no Kaspersky Security Center

Caso ocorra um problema ao operar o Kaspersky Embedded Systems Security for Windows (por exemplo, o aplicativo travar), é possível diagnosticá-lo. Para fazer isso, é possível ativar a criação de arquivos de rastreamento e um arquivo de despejo para o processo do Kaspersky Embedded Systems Security for Windows e enviar esses arquivos para análise ao Suporte Técnico.

O Kaspersky Embedded Systems Security for Windows não envia nenhum arquivo de rastreamento ou de despejo automaticamente. Os dados de diagnóstico só podem ser enviados por um usuário com as permissões necessárias.

O Kaspersky Embedded Systems Security for Windows grava as informações nos arquivos de rastreamento e no arquivo de despejo no formulário 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 for Windows. É possível configurar as permissões de acesso e permitir que apenas os usuários necessários acessem os logs, arquivos de rastreamento e de despejo.

Para definir configurações de diagnóstico de travamento no Kaspersky Security Center:

1. No Console de Administração do Kaspersky Security Center, abra a janela **Configurações do aplicativo**.
2. Abra a seção **Diagnóstico de mau funcionamento**.
3. Para registrar informações de depuração em um arquivo, na seção **Configurações de solução de problemas**, marque a caixa de seleção **Ativar rastreamento**.
4. No campo **Pasta para rastreamento de arquivos**, especifique o caminho absoluto para uma pasta local onde o Kaspersky Embedded Systems Security for Windows salvará os arquivos de rastreamento.

   A pasta deve ser criada com antecedência e deve ter permissão de gravação pela conta SYSTEM. Não é possível especificar uma pasta de rede, uma unidade ou variáveis de ambiente.
5. Configure o nível de detalhe das informações de depuração.
6. Especifique o **Tamanho máximo de arquivos de rastreamento (MB)**.

   Valores disponíveis: de 1 a 4095 MB. Por padrão, o tamanho máximo dos arquivos de rastreamento é definido como 50 MB.
7. Para excluir os arquivos de rastreamento mais antigos quando o número máximo de arquivos for atingido, marque a caixa de seleção **Remover os arquivos de rastreamento mais antigos**.
8. Especifique o **Número máximo de arquivos para um log de rastreamento**.

   Valores disponíveis: de 1 a 999. Por padrão, o número máximo de arquivos é cinco. O campo estará disponível se a caixa de seleção **Remover os arquivos de rastreamento mais antigos** estiver marcada.
9. Se desejar que o aplicativo crie um arquivo de despejo, selecione a caixa **Criar arquivo de despejo**.
10. No campo **Pasta de arquivos de despejo**, especifique o caminho absoluto para uma pasta local onde o Kaspersky Embedded Systems Security for Windows salvará o arquivo de despejo.

    A pasta deve ser criada com antecedência e deve ter permissão de gravação pela conta SYSTEM. Não é possível especificar uma pasta de rede, uma unidade ou variáveis de ambiente.
11. Clique no botão **OK**.

As configurações do aplicativo definidas são aplicadas no dispositivo protegido.

Gerenciando programações de tarefas

É possível programar as tarefas do Kaspersky Embedded Systems Security for Windows.

Programação de tarefas

É possível programar tarefas locais do sistema e tarefas personalizadas no Console do Aplicativo. Não é possível programar tarefas de grupo no Console do Aplicativo.

Para programar tarefas de grupo utilizando o Plug-in de Administração:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados**.
2. Selecione o grupo ao qual o dispositivo protegido pertence.
3. No painel de resultados, selecione a guia **Tarefas**.
4. Abra a janela **Propriedades: <Nome da tarefa>** usando uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa.
   - Abra o menu de contexto do nome da tarefa e selecione o item Propriedades.
5. Selecione a seção **Agendamento**.
6. No bloco **Configurações de agendamento**, marque a caixa de seleção **Executar de acordo com o agendamento**.

   Os campos com configurações de programação para as tarefas de Verificação por Demanda e de Atualização estarão indisponíveis caso a programação dessas tarefas seja bloqueada por uma política do Kaspersky Security Center.

7. 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 nos quais a tarefa será iniciada (por padrão, as tarefas são executadas nas segundas-feiras).
      - **Ao iniciar o aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security for Windows.
      - **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 quando a programação inicia.

      Depois de programar a hora e data de início e a frequência da tarefa, a hora estimada para a próxima execução é exibida.

Acesse a guia **Agendamento** e abra a janela **Configurações de tarefa**. No campo **Próxima execução** na parte superior da janela, a hora de inicialização estimada é exibida. Cada vez que a janela é aberta, essa hora de início estimada é atualizada e exibida.

O campo **Próxima execução** exibe o valor **Bloqueado pela política** caso as configurações de política ativa do Kaspersky Security Center proíbam a execução de tarefas locais do sistema programadas.

8. 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, nos campos à direita, insira o número máximo de horas e minutos da execução da tarefa.

     b. Marque a caixa de seleção **Pausar de** e, nos campos à direita, insira os valores iniciais e finais de um intervalo de tempo menor que 24 horas durante o qual a execução da tarefa será pausada.

   - No bloco **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 **Randomizar a hora de início da tarefa no intervalo de** e especifique um valor em minutos.

9. Clique no botão **OK**.

10. Clique no botão **Aplicar** para salvar as configurações de início da tarefa.

Caso queira definir as configurações do aplicativo para uma única tarefa usando o Kaspersky Security Center, acesse a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center".

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 inicialização da tarefa:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados**.

2. Selecione o grupo ao qual o dispositivo protegido pertence.

3. No painel de resultados, selecione a guia **Tarefas**.

4. Abra a janela **Propriedades: <Nome da tarefa>** usando uma das seguintes maneiras:

- Clique duas vezes no nome da tarefa.
- Abra o menu de contexto do nome da tarefa e selecione o item Propriedades.

5. Selecione a seção **Agendamento**.
6. Execute uma das seguintes ações:
   - Marque a caixa de seleção **Executar de acordo com o agendamento** se desejar ativar a programação de inicialização da tarefa.
   - Desmarque a caixa de seleção **Executar de acordo com o agendamento** se desejar desativar a programação de inicialização da tarefa.

     As configurações da programação de inicialização da tarefas não são excluídas e serão aplicadas na próxima vez que a inicialização programada de uma tarefa for ativada.
7. Clique no botão **OK**.
8. Clique no botão **Aplicar**.

As definições de programação de inicialização da tarefa configuradas são salvas.

Relatórios no 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 for Windows:

- 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 sobre o status de componentes do Kaspersky Embedded Systems Security for Windows

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: *Em execução*, *Pausado*, *Interrompido*, *Mau funcionamento*, *Não instalado*, *Iniciando*.

O status *Não instalado* refere-se ao componente, não ao próprio aplicativo. Caso o aplicativo não esteja 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 um conjunto de componentes especificado 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 do componente nas configurações do aplicativo:

1. Expanda o node **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**.
3. Selecione a seção **Componentes**.
4. Revise a tabela de status.

Para revisar um relatório padrão do Kaspersky Security Center:

1. Selecione o node **Servidor de Administração <Nome do Servidor de Administração>** 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 proibidos nos modos Ativa e de teste

Com base nos resultados da tarefa de Controle de Inicialização de Aplicativos, dois tipos de relatórios podem ser gerados: o relatório de aplicativos proibidos (se a tarefa for iniciada no modo Ativa) e um 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 dispositivos protegidos da rede. Cada relatório é gerado para todos os grupos de administração e acumula dados de todos os aplicativos da Kaspersky instalados nos dispositivos protegidos.

Para revisar um relatório de aplicativos proibidos no modo Somente Estatísticas:

1. Inicie a tarefa de Controle de Inicialização de Aplicativos no modo Somente estatísticas.

Selecione o node **Servidor de Administração <Nome do Servidor de Administração>** na árvore do Console de Administração.

1. Abra a guia **Relatórios**.
2. Clique duas vezes no item **Relatório de aplicativos proibidos em modo de teste**.

   Um relatório é gerado.
3. Revise os seguintes detalhes do relatório:

   - Um diagrama gráfico que exibe os 10 aplicativos com o maior número de inicializações bloqueadas.
   - Uma tabela de resumo de bloqueios de aplicativos 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 Ativa:

1. Inicie a tarefa de Controle de Inicialização de Aplicativos no modo Ativa.
2. Selecione o node **Servidor de Administração <Nome do Servidor de Administração>** na árvore do Console de Administração.
3. Abra a guia **Relatórios**.
4. Clique duas vezes no item **Relatório de aplicativos proibidos**.

   Um relatório é gerado.

Este relatório contém os mesmos dados sobre blocos que o relatório de aplicativos proibidos no modo de teste.

Trabalhar com o Console do Kaspersky Embedded Systems Security for Windows

Esta seção fornece informações sobre o Console do Kaspersky Embedded Systems Security for Windows e descreve como gerenciar o aplicativo usando o Console do Aplicativo instalado no dispositivo protegido ou em outro dispositivo.

Sobre o Console do Kaspersky Embedded Systems Security for Windows

O Console do Kaspersky Embedded Systems Security for Windows é um snap-in isolado que pode ser adicionado ao Console de Gerenciamento Microsoft.

O aplicativo pode ser gerenciado por meio do Console do Aplicativo instalado no dispositivo protegido ou em outro dispositivo na rede corporativa.

Depois que o Console do Aplicativo for instalado em outro dispositivo, é necessária uma configuração avançada.

É possível instalar o Console do Aplicativo e o Kaspersky Embedded Systems Security for Windows em diferentes dispositivos protegidos atribuídos a diferentes domínios. Nesse caso, pode haver limitações quanto ao envio de informações a partir do aplicativo para o Console do Aplicativo. Por exemplo, após o início de uma tarefa de aplicativo, seu status pode permanecer inalterado no Console do Aplicativo.

Ao instalar o Console do Aplicativo, o assistente de instalação cria o arquivo kavfs.msc na pasta instalação e adiciona o snap-in do Kaspersky Embedded Systems Security for Windows à lista de snap-ins isolados do Microsoft Windows.

Você pode iniciar o Console do Aplicativo do menu **Iniciar**. O arquivo msc do snap-in do Kaspersky Embedded Systems Security for Windows pode ser executado ou adicionado ao Console de Gerenciamento Microsoft como um novo elemento na árvore.

Em uma versão de 64 bits do Microsoft Windows, o snap-in do Kaspersky Embedded Systems Security for Windows pode ser adicionado somente na versão de 32 bits do Console de Gerenciamento Microsoft. Para adicionar o snap-in do Kaspersky Embedded Systems Security for Windows, abra o Console de Gerenciamento Microsoft a partir da linha de comando executando o comando: mmc.exe /32.

Vários snap-ins do Kaspersky Embedded Systems Security for Windows podem ser adicionados a um Console de Gerenciamento Microsoft aberto no modo autor. É possível então gerenciar a proteção de vários dispositivos nos quais o Kaspersky Embedded Systems Security for Windows está instalado.

Interface do Console do Kaspersky Embedded Systems Security for Windows

Esta seção descreve os elementos primários da interface do aplicativo.

Janela do Console do Kaspersky Embedded Systems Security for Windows

O Kaspersky Embedded Systems Security for Windows Console é exibido como um nó na árvore do Microsoft Management Console.

Após estabelecer uma conexão com o Kaspersky Embedded Systems Security for Windows instalado em um dispositivo protegido diferente, o nome do nó será complementado com o nome do dispositivo protegido no qual o aplicativo está instalado e o nome da conta de usuário com a qual a conexão foi estabelecida: **Kaspersky Embedded Systems Security for Windows <Nome do dispositivo protegido> como <nome da conta>**. Ao conectar o Kaspersky Embedded Systems Security for Windows instalado no mesmo dispositivo protegido com o Console do Aplicativo, o nome do nó será **Kaspersky Embedded Systems Security for Windows**.

A árvore do Console do Aplicativo

A árvore do Console do Aplicativo exibe o node **Kaspersky Embedded Systems Security for Windows** e os subnós dos componentes funcionais do aplicativo.

O nó **Kaspersky Embedded Systems Security for Windows** inclui os seguintes subnós:

- **Proteção do Computador em Tempo Real**: gerencia tarefas de Proteção do Computador em Tempo Real e serviços da KSN. O nó **Proteção do Computador em Tempo Real** permite configurar as seguintes tarefas:
  - **Proteção de Arquivos em Tempo Real**
  - **Uso da KSN**
  - **Prevenção de Exploits**
- **Controle do Computador**: controle de aplicativos em execução no dispositivo protegido e nos dispositivos conectados. O nó **Controle do Computador** permite configurar as seguintes tarefas:
  - **Controle de Inicialização de Aplicativos**
  - **Controle de Dispositivos**
  - **Gerenciamento de firewall**
- **Geradores de regras automatizadas**: a configuração de geração automática de regras de grupo e de sistema para as tarefas de Controle de Inicialização de Aplicativos e Controle de Dispositivos.
  - **Gerador de Regras de Controle de Inicialização de Aplicativos**
  - **Gerador de Regras de Controle de Dispositivos**
  - Tarefas de grupo de geração de regras **<Nomes das tarefas>** (se aplicável)

    As tarefas de grupo são criadas usando o Kaspersky Security Center. Você não pode gerenciar tarefas de grupo pelo Console do Aplicativo.
- **Inspeção do sistema**: configuração do controle de operações de arquivos e configurações de inspeção do Log de Eventos do Windows.
  - **Monitor de Integridade de Arquivos**
  - **Inspeção do Log**
- **Verificação por demanda**: gerencia as tarefas de Verificação por Demanda. Existe um nó separado para cada tarefa:

- **Verificação na Inicialização do Sistema Operacional**
- **Verificação de Áreas Críticas**
- **Verificação da Quarentena**
- **Controle de Integridade de Aplicativos**
- Tarefas personalizadas **<Nomes das tarefas>** (se aplicável)

O nó exibe tarefas do sistema criadas quando o aplicativo é instalado, tarefas personalizadas e de Verificação por Demanda de grupo criadas e enviadas para um dispositivo protegido usando o Kaspersky Security Center.

- **Atualização**: gerencia as atualizações dos bancos de dados e dos módulos do Kaspersky Embedded Systems Security for Windows e copia a atualização em uma pasta de fonte de atualização local. O nó contém nós secundários para administrar cada tarefa de atualização e a última tarefa de **Reversão da atualização do banco de dados do aplicativo**:
  - **Atualização do Banco de Dados**
  - **Atualização dos Módulos de Software**
  - **Copiar atualizações**
  - **Reversão da atualização do banco de dados do aplicativo**

  O nó exibe todas as tarefas de atualização de grupo e personalizadas criadas e enviadas a um dispositivo protegido usando o Kaspersky Security Center.
- **Armazenamentos**: Gerenciamento das configurações de Quarentena e de Backup.
  - **Quarentena**
  - **Backup**
- **Logs e notificações**: gerencia logs de tarefas locais, log de segurança e log de auditoria do Sistema Kaspersky Embedded Systems Security for Windows.
  - **Log de segurança**
  - **Log de auditoria do sistema**
  - **Logs de tarefas**
- **Licenciamento**: adiciona ou exclui as chaves do Kaspersky Embedded Systems Security for Windows e exibe os detalhes da licença.

Painel de detalhes

O painel de detalhes exibe informações sobre o node selecionado. Caso o nó do **Kaspersky Embedded Systems Security for Windows** seja selecionado, o painel de detalhes exibe as informações sobre o status de proteção do dispositivo atual e sobre o Kaspersky Embedded Systems Security for Windows, o status de proteção dos seus componentes funcionais e a data de expiração da licença.

Menu de contexto do node Kaspersky Embedded Systems Security for Windows

Você pode usar os itens do menu de contexto do node do **Kaspersky Embedded Systems Security for Windows** para executar as seguintes operações:

- **Conectar a outro computador**. Conectar a outro dispositivo para gerenciar o Kaspersky Embedded Systems Security for Windows instalado nele. Você também pode executar esta operação clicando no link no canto inferior direito do painel de detalhes do node **Kaspersky Embedded Systems Security for Windows**.
- **Iniciar o serviço/Parar o serviço**. Iniciar ou interromper o aplicativo ou uma tarefa selecionada. Para executar essas operações, você também pode usar os botões da barra de ferramentas. Você também pode executar estas operações nos menus de contexto de tarefas do aplicativo.
- **Configurar verificação de unidades removíveis**. Configurar a verificação de unidades removíveis conectadas ao dispositivo protegido via porta USB.
- **Configurar a Zona Confiável**. Visualize e defina as configurações da Zona Confiável.
- **Modificar direitos de gerenciamento de aplicativos do usuário**. Visualize e configure permissões de acesso a funções do Kaspersky Embedded Systems Security for Windows.
- **Modificar direitos do usuário de gerenciamento do Kaspersky Security Service**. Visualize e configure direitos de usuário para gerenciar Kaspersky Security Service.
- **Exportar configurações**. Salve as configurações do aplicativo em um arquivo de configuração no formato XML. Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.
- **Importar configurações**. Importe configurações do aplicativo de um arquivo de configuração no formato XML. Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.
- **Informações sobre o aplicativo e atualizações de módulo disponíveis**. Consultar as informações sobre o Kaspersky Embedded Systems Security for Windows e as atualizações dos módulos de software disponíveis atualmente.
- **Atualizar**. Atualize o conteúdo da janela de Console do Aplicativo. Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.
- **Propriedades**. Visualize e defina as configurações do Kaspersky Embedded Systems Security for Windows ou uma tarefa selecionada. Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.

  Para fazer isso, você também pode usar o link **Propriedades do aplicativo** no painel de detalhes do node do **Kaspersky Embedded Systems Security for Windows** ou usar o botão na barra de ferramentas.

- **Ajuda**. Visualize as informações na Ajuda do Kaspersky Embedded Systems Security for Windows. Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.

Barra de ferramentas e menu de contexto das tarefas do Kaspersky Embedded Systems Security for Windows

É possível gerenciar as tarefas do Kaspersky Embedded Systems Security for Windows usando os itens dos menus de contexto de cada tarefa na árvore do Console do Aplicativo.

Você pode usar os itens do menu de contexto para executar as seguintes operações:

- **Iniciar/Interromper**. Inicie ou interrompa a execução de uma tarefa. Para executar essas operações, você também pode usar os botões da barra de ferramentas.
- **Reiniciar/Pausar**. Reinicie ou pause a execução de uma tarefa. Para executar essas operações, você também pode usar os botões da barra de ferramentas. Esta operação está disponível para as tarefas de Proteção do Computador em Tempo Real e tarefas de Verificação por Demanda.
- **Adicionar tarefa**. Crie uma nota tarefa personalizada. Esta operação está disponível para tarefas de Verificação por Demanda.
- **Abrir log**. Visualizar e gerenciar o log de tarefas. Esta operação está disponível para todas as tarefas.
- **Remover tarefa**. Excluir tarefa personalizada. Esta operação está disponível para tarefas de Verificação por Demanda.
- **Modelos de configurações**. Gerencie modelos. Esta operação está disponível para a Proteção de Arquivos em Tempo Real e a Verificação por Demanda.

Ícone da Bandeja do Sistema na área de notificação

Cada vez que o Kaspersky Embedded Systems Security for Windows é iniciado automaticamente depois de uma reinicialização do dispositivo protegido, o ícone da bandeja do sistema é exibido na área de notificação da barra de ferramentas . Ele é exibido por padrão se o componente do ícone da bandeja do sistema tiver sido instalado durante a configuração do aplicativo.

A aparência do ícone da bandeja do sistema reflete o status de proteção atual do dispositivo. Existem dois tipos de status:

	Ativo (ícone colorido), se pelo menos uma das tarefas estiver sendo executada: Proteção de Arquivos em Tempo Real, Controle de Inicialização de Aplicativos.
	Inativo (ícone em cinza) – nenhuma das seguintes tarefas está sendo executada no momento: Proteção de Arquivos em Tempo Real e Controle de Inicialização de Aplicativos

Você pode abrir o menu de contexto do ícone da bandeja de sistema clicando nele com o botão direito do mouse.

O menu de contexto oferece vários comandos para exibir as janelas do aplicativo (consulte a tabela abaixo).

Comandos do menu de contexto no ícone da bandeja do sistema

Comando	Descrição
Abrir o Console do Aplicativo	Abre o Console do Kaspersky Embedded Systems Security for Windows (se instalado).
Abrir Interface de diagnóstico compacta	Abre a interface de diagnóstico compacta.
Sobre o aplicativo	Abre a janela **Sobre o aplicativo**, que contém informações sobre o Kaspersky Embedded Systems Security for Windows. Para usuários registrados do Kaspersky Embedded Systems Security for Windows, a janela **Sobre o aplicativo** inclui as informações sobre atualizações urgentes que tenham sido instaladas.
Ocultar	Oculta o ícone da bandeja de sistema na área de notificação da barra de ferramentas.

Você pode exibir o ícone oculto da bandeja do sistema novamente a qualquer momento.

Para exibir o ícone da bandeja do sistema novamente,

no menu **Iniciar** do Microsoft Windows, selecione **Todos os Programas** > **Kaspersky Embedded Systems Security for Windows** > **Ícone na bandeja do sistema**.

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

Nas configurações gerais do Kaspersky Embedded Systems Security for Windows, é possível ativar ou desativar a exibição do ícone da bandeja do sistema sempre que o aplicativo for iniciado automaticamente após uma reinicialização do dispositivo protegido.

Gerenciamento do Kaspersky Embedded Systems Security for Windows por meio do Console do Aplicativo em outro dispositivo

É possível gerenciar o Kaspersky Embedded Systems Security for Windows por meio do Console do Aplicativo instalado em um dispositivo remoto.

Para gerenciar o aplicativo utilizando o Console do Kaspersky Embedded Systems Security for Windows em um dispositivo remoto, certifique-se de que:

- Os usuários do Console do Aplicativo no dispositivo remoto sejam adicionados ao grupo de Administradores de ESS no dispositivo protegido.
- As conexões de rede são permitidas para o processo do Kaspersky Security Management Service (kavfsgt.exe) se o Firewall do Windows estiver ativado no dispositivo protegido.
- Durante a instalação do Kaspersky Embedded Systems Security for Windows, a caixa de seleção **Permitir acesso remoto** é marcada na janela do Assistente de instalação.

Caso o Kaspersky Embedded Systems Security for Windows no dispositivo remoto seja protegido por senha, insira a senha para acessar o gerenciamento de aplicativos por meio do Console do Aplicativo.

Definição das configurações gerais do aplicativo por meio do Console do Aplicativo

As configurações gerais e as configurações de diagnóstico de mau funcionamento das configurações do Kaspersky Embedded Systems Security for Windows estabelecem as condições gerais nas quais o aplicativo opera. Essas configurações permitem controlar o número de processos de trabalho usados pelo Kaspersky Embedded Systems Security for Windows, ativar a recuperação de tarefas do Kaspersky Embedded Systems Security for Windows após um encerramento anormal, manter o log, ativar a criação de arquivos de despejo dos processos do Kaspersky Embedded Systems Security for Windows após um encerramento anormal e definir outras configurações gerais.

As configurações do aplicativo não podem ser definidas no Console do Aplicativo se a política ativa do Kaspersky Security Center bloquear alterações a essas configurações.

Para definir as configurações do Kaspersky Embedded Systems Security for Windows:

1. Na árvore do Console do Aplicativo, selecione o node **Kaspersky Embedded Systems Security for Windows** e execute uma das seguintes ações:

   - Clique no link **Propriedades do aplicativo** no painel de detalhes do node.
   - Selecione **Propriedades** no cardápio de contexto do node.

   A janela **Configurações do aplicativo** é exibida.

2. Na janela exibida, especifique as configurações gerais do Kaspersky Embedded Systems Security for Windows de acordo com suas preferências:

   - As seguintes configurações podem ser especificadas na guia **Escalabilidade e interface**:
     - Na seção **Configurações de escalabilidade**:
       - Número de processos para a Proteção do Computador em Tempo Real
       - Número de processos de trabalho para tarefas de Verificação por Demanda em segundo plano
   - Na seção **Interação com o usuário**, selecione se o Ícone da Bandeja do Sistema será exibido na barra de tarefas após a inicialização de cada aplicativo.
   - As configurações seguintes podem ser especificadas na guia **Segurança e confiabilidade**:
     - Na seção **Configurações de proteção de senha**, configure a proteção de processos do aplicativo.
     - Na seção **Configurações de proteção de senha**, defina as configurações de proteção por senha das funções do aplicativo.
     - Na seção **Autodefesa**, especifique o número de tentativas para recuperar uma tarefa de Verificação por Demanda caso ocorra travamento.
   - Na seção **Recupere tarefas de verificação por demanda não mais do que (vezes)**, especifique as ações que o Kaspersky Embedded Systems Security for Windows realizará quando mudar para a energia UPS.
   - Na guia **Configurações de verificação**:
     - **Restaurar os atributos do arquivo após a verificação**
     - **Limitar a utilização da CPU para threads de verificação**
     - **Limite superior (porcento)**
     - **Pasta para os arquivos temporários criados durante a verificação**
   - Na guia **Configurações de conexão**:
     - Na seção **Configurações do servidor proxy**, especifique as configurações do servidor proxy.
     - Na seção **Configurações de autenticação do servidor proxy**, especifique o tipo de autenticação e detalhes exigidos para a autenticação no servidor proxy.

- Na seção **Licenciamento**, indique se o Kaspersky Security Center será utilizado como um servidor proxy para a ativação do aplicativo.

- Na guia **Diagnóstico de mau funcionamento**:

  - Caso deseje que o aplicativo grave as informações de depuração em um arquivo, na subseção **Configurações de solução de problemas**, marque a caixa de seleção **Ativar o rastreamento**.

  - No campo **Pasta de rastreamento**, especifique o caminho absoluto para uma pasta local onde o Kaspersky Embedded Systems Security for Windows salvará os arquivos de rastreamento.

    A pasta deve ser criada com antecedência e deve ter permissão de gravação pela conta SYSTEM. Não é possível especificar uma pasta de rede, uma unidade ou variáveis de ambiente.

  - Configure o nível de detalhe das informações de depuração.

  - Especifique o **Tamanho máximo dos arquivos de rastreamento**.

    Valores disponíveis: de 1 a 4095 MB. Por padrão, o tamanho máximo dos arquivos de rastreamento é definido como 50 MB.

  - Caso deseje que o aplicativo remova os arquivos mais antigos após o número máximo de arquivos de rastreamento ser atingido, marque a caixa de seleção **Remover os arquivos de rastreamento mais antigos**.

  - Especifique o **Número máximo de arquivos para um log de rastreamento**.

    Valores disponíveis: de 1 a 999. Por padrão, o número máximo de arquivos é cinco. O campo estará disponível apenas se a caixa de seleção **Remover os arquivos de rastreamento mais antigos** estiver marcada.

  - Se desejar que o aplicativo crie um arquivo de despejo, selecione a caixa **Criar arquivo de despejo**.

  - No campo **Pasta de arquivos de despejo**, especifique o caminho absoluto para uma pasta local onde o Kaspersky Embedded Systems Security for Windows salvará o arquivo de despejo.

    A pasta deve ser criada com antecedência e deve ter permissão de gravação pela conta SYSTEM. Não é possível especificar uma pasta de rede, uma unidade ou variáveis de ambiente.

O Kaspersky Embedded Systems Security for Windows grava as informações nos arquivos de rastreamento e no arquivo de despejo no formulário 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 for Windows. É possível configurar as permissões de acesso e permitir que apenas os usuários necessários acessem os logs, arquivos de rastreamento e de despejo.

3. Clique no botão **OK**.

As configurações do Kaspersky Embedded Systems Security for Windows são salvas.

Gerenciando as tarefas do Kaspersky Embedded Systems Security for Windows

Esta seção contém informações sobre como criar, configurar, iniciar e interromper as tarefas do Kaspersky Embedded Systems Security for Windows.

Categorias de tarefa do Kaspersky Embedded Systems Security for Windows

A Proteção do Computador em Tempo Real, o Controle do Computador, a Verificação por Demanda e as funções de Atualização no Kaspersky Embedded Systems Security for Windows são implementadas como tarefas.

É possível gerenciar as tarefas utilizando o menu de contexto da tarefa na árvore do Console do Aplicativo, a barra de ferramentas e a barra de acesso rápido. É possível visualizar as informações de status painel de resultados. As operações de gerenciamento de tarefas são gravadas no log de auditoria do sistema.

Há dois tipos de tarefas do Kaspersky Embedded Systems Security for Windows: *local* e *grupo*.

Tarefas locais

As tarefas locais só podem ser executadas no dispositivo protegido para o qual foram criadas. Dependendo do método de início, há os seguintes tipos de tarefas locais:

- **Tarefas locais do sistema**. As tarefas são criadas automaticamente durante a instalação do Kaspersky Embedded Systems Security for Windows. Você pode editar as configurações de todas as tarefas locais do sistema, exceto as tarefas de Verificação da Quarentena e Reversão da Atualização do Banco de Dados. As tarefas locais do sistema não podem ser renomeadas ou excluídas. É possível executar tarefas de Verificação por Demanda do sistema e personalizadas simultaneamente.

- **Tarefas locais personalizadas**. No Console do Aplicativo, você pode criar tarefas de Verificação por Demanda. No Kaspersky Security Center, é possível criar tarefas de Verificação sob Demanda, Atualização do Banco de Dados, Reversão da Atualização do Banco de Dados e Copiar Atualizações. É possível renomear, configurar e excluir tarefas personalizadas. É possível executar várias tarefas personalizadas simultaneamente.

Tarefas de grupo

É possível gerenciar tarefas de grupo e tarefas para conjuntos de dispositivos protegidos a partir do Kaspersky Security Center. Todas as tarefas de grupo são tarefas personalizadas. As tarefas de grupo também são exibidas no Console do Aplicativo. No Console do Aplicativo, você pode visualizar somente o status de tarefas de grupo. Não é possível utilizar o Console do Aplicativo para gerenciar ou configurar tarefas de grupo.

Executar, pausar, reiniciar e interromper tarefas manualmente

Você pode fazer uma pausa e reiniciar somente as tarefas de Proteção do Computador em Tempo Real e de Verificação por Demanda. Nenhuma outra tarefa pode ser pausada ou reiniciada manualmente.

Para iniciar, pausar, reiniciar ou interromper uma tarefa:

1. No Console do Aplicativo, abra o menu de contexto da tarefa.

2. Selecione um dos seguintes comandos: **Iniciar**, **Pausar**, **Reiniciar** ou **Interromper**.

A operação é executada e registrada no log de auditoria do sistema.

Quando uma tarefa de Verificação por Demanda é reiniciada, o Kaspersky Embedded Systems Security for Windows reinicia a verificação a partir do objeto no qual a verificação foi pausada.

Gerenciando programações de tarefas

É possível programar as tarefas do Kaspersky Embedded Systems Security for Windows.

Definição das configurações da programação da tarefa

No Console do Aplicativo, é possível programar o início de tarefas locais do sistema e tarefas personalizadas. No entanto, não é possível programar o início de tarefas de grupo.

Para programar uma tarefa:

1. Abra o menu de contexto da tarefa que deseja programar.
2. Selecione **Propriedades**.
   A janela **Configurações de tarefa** é aberta.
3. Na janela exibida, na guia **Agendamento**, marque a caixa de seleção **Executar de acordo com o agendamento**.
4. Siga estas etapas para especificar as configurações de programação:
   a. No menu suspenso **Frequência**, selecione uma das seguintes opções:
      - **De hora em hora**: para executar a tarefa em intervalos medidos em horas; especifique o número de horas no campo **A cada<número>hora(s)**.
      - **Diariamente**: para executar a tarefa em intervalos diários; especifique o número de dias no campo **A cada<número>dia(s)**.
      - **Semanalmente**: para executar a tarefa em intervalos semanais; especifique o número de semanas no campo **A cada<número>semana(s) em**. Especifique os dias da semana nos quais a tarefa será iniciada (por padrão, as tarefas são executadas nas segundas-feiras).
      - **Ao iniciar o aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security for Windows.
      - **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 em que a tarefa será iniciada pela primeira vez.

Após ter especificado a frequência de início da tarefa, a hora da primeira inicialização e a data a partir da qual a programação será aplicada, a hora estimada para a próxima inicialização da tarefa será exibida na parte superior da janela, no campo **Próxima execução**. A hora estimada da próxima execução da tarefa será atualizada e exibida sempre que você abrir a janela **Configurações de tarefa** na guia **Agendamento**.

O campo **Próxima execução** exibe o valor **Bloqueado pela política** caso as configurações de política ativa do Kaspersky Security Center proíbam a execução de tarefas locais do sistema programadas.

5. Utilize a guia **Avançado** para especificar as seguintes configurações de programação:

   - Na seção **Configurações de interrupção de tarefa**:

     a. Marque a caixa de seleção **Duração**. Nos campos à direita, insira a duração máxima da tarefa em horas e minutos.

     b. Marque a caixa de seleção **Pausar de**. Nos campos à direita, insira quando pausar e reiniciar a tarefa (menos de 24 horas).

   - No bloco **Configurações avançadas**:

     a. Marque a caixa de seleção **Cancelar agendamento a partir de** e especifique a data de término da programação da tarefa.

     b. Marque a caixa de seleção **Executar tarefas ignoradas** para inicializar as tarefas ignoradas.

     c. Marque a caixa de seleção **Aleatorizar o início da tarefa dentro do intervalo de** e especifique um valor em minutos.

6. Clique no botão **OK**.

As configurações de programação da tarefa são salvas.

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 o início de uma tarefa programada:

1. Na árvore do Console do Aplicativo, abra o menu de contexto para a tarefa programada.
2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é aberta.
3. Na janela aberta, na guia **Agendamento**, selecione uma das seguintes opções:

   - Marque a caixa de seleção **Executar de acordo com o agendamento** se desejar ativar a programação de inicialização da tarefa.
   - Desmarque a caixa de seleção **Executar de acordo com o agendamento** se desejar desativar a programação de inicialização da tarefa.

As configurações da programação de inicialização da tarefa não são excluídas e serão aplicadas na próxima vez que a inicialização programada de uma tarefa for ativada.

4. Clique no botão **OK**.

As configurações de programação da tarefa são salvas.

Uso de contas de usuário para iniciar tarefas

É possível iniciar tarefas na conta do sistema ou especificar uma conta diferente.

Sobre como usar contas para iniciar tarefas

É possível especificar a conta para executar as seguintes tarefas do Kaspersky Embedded Systems Security for Windows:

- Gerador de Regras de Controle de Inicialização de Aplicativos
- Gerador de Regras de Controle de Dispositivos
- Verificação por Demanda
- Atualização

Por padrão, essas tarefas são executadas usando as permissões de conta do sistema.

Uma conta diferente com as permissões de acesso apropriadas é recomendada nos seguintes casos:

- Tarefa de **atualização**: caso tenha especificado uma pasta compartilhada em outro dispositivo na rede como fonte de atualização.
- Tarefa de **atualização**: caso um servidor proxy com a autenticação NTLM incluída no Windows for utilizado para acessar a fonte de atualização.
- Tarefas de **Verificação por Demanda**: caso a conta do sistema não tenha as permissões para acessar qualquer os objetos verificados (por exemplo, arquivos em pastas compartilhadas no dispositivo protegido).
- Tarefa do **Gerador de Regras de Controle de Inicialização de Aplicativos**: caso as regras geradas tenham sido exportadas para um arquivo de configuração que a conta do sistema não possa acessar (por exemplo, em uma pasta compartilhada no dispositivo protegido).

É possível executar as tarefas de Atualização, de Verificação por Demanda e do Gerador de Regras de Controle de Inicialização de Aplicativos com as permissões de conta do sistema. O Kaspersky Embedded Systems Security for Windows executa essas tarefas e acessa as pastas compartilhadas em outro dispositivo na rede caso o dispositivo esteja registrado no mesmo domínio do dispositivo protegido. Nesse caso, a conta do sistema deve possuir permissões de acesso para as pastas. O Kaspersky Embedded Systems Security for Windows acessará o dispositivo utilizando as permissões da conta **<nome do domínio \ nome_do_dispositivo>**.

Especificação de uma conta de usuário para iniciar uma tarefa

Para especificar uma conta para iniciar uma tarefa:

1. Na árvore do Console do Aplicativo, abra o menu de contexto da tarefa que deseja iniciar utilizando uma conta específica.
2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é aberta.
3. Na janela aberta, na guia **Executar como**, siga estas etapas:

   a. Selecione **Nome de usuário**.

   b. Insira o nome de usuário e a senha para a conta que você deseja usar.

   > O usuário selecionado deve estar registrado no dispositivo protegido ou no mesmo domínio que esse computador.

   c. Confirme a senha.
4. Clique no botão **OK**.

As configurações modificadas são salvas.

Configurações de importação e exportação

Esta seção explica como exportar as configurações do Kaspersky Embedded Systems Security for Windows. Você também aprenderá como exportar configurações de software específicas para um arquivo de configuração XML e como importar essas configurações de um arquivo de configuração de volta para o aplicativo.

Sobre a importação e exportação de configurações

Você pode exportar as configurações do Kaspersky Embedded Systems Security for Windows para um arquivo de configuração XML e importar configurações para o Kaspersky Embedded Systems Security for Windows a partir do arquivo de configuração. É possível salvar todas as configurações do aplicativo ou apenas aquelas de componentes individuais como um arquivo de configuração.

Quando você exporta todas as configurações do Kaspersky Embedded Systems Security for Windows a um arquivo, as configurações gerais do aplicativo e as configurações dos seguintes componentes e funções do Kaspersky Embedded Systems Security for Windows são salvas:

- Proteção de Arquivos em Tempo Real
- Uso da KSN
- Controle de Dispositivos

- Controle de Inicialização de Aplicativos
- Gerador de Regras de Controle de Dispositivos
- Gerador de Regras de Controle de Inicialização de Aplicativos
- Tarefas de Verificação por Demanda
- Monitor de Integridade de Arquivos
- Inspeção do Log
- Atualização do banco de dados e dos módulos de software do Kaspersky Embedded Systems Security for Windows
- Quarentena
- Backup
- Logs
- Notificações do administrador e dos usuários
- Zona confiável
- Prevenção de Exploits
- Proteção por senha

Além disso, você pode salvar as configurações gerais do Kaspersky Embedded Systems Security for Windows no arquivo, bem como os direitos das contas de usuário.

Não é possível exportar as configurações de tarefas de grupo.

O Kaspersky Embedded Systems Security for Windows exporta todas as senhas usadas pelo aplicativo, por exemplo, as configurações da conta de usuário para executar tarefas ou conectar-se a um servidor proxy. As senhas exportadas são salvas na forma criptografada do arquivo de configuração. É possível importar senhas usando apenas o Kaspersky Embedded Systems Security for Windows instalado nesse dispositivo protegido caso não tenha sido reinstalado ou atualizado.

Não é possível importar senhas salvas anteriormente usando o Kaspersky Embedded Systems Security for Windows instalado em um dispositivo protegido diferente. Depois que as configurações tiverem sido importadas no dispositivo protegido, todas as senhas deverão ser inseridas manualmente.

Se uma política do Kaspersky Security Center estiver ativa no momento da exportação, o aplicativo exportará os valores especificados usados por essa política.

As definições podem ser importadas de um arquivo de configuração contendo definições para os componentes individuais do Kaspersky Embedded Systems Security for Windows (por exemplo, um arquivo criado no Kaspersky Embedded Systems Security for Windows instalado com um conjunto incompleto de componentes). Depois que as configurações são importadas, somente estas configurações do Kaspersky Embedded Systems Security for Windows que estavam contidas no arquivo de configuração serão alteradas. Todas as outras configurações permanecem iguais.

As configurações de uma política ativa do Kaspersky Security Center que tenham sido bloqueadas não são alteradas ao importar as configurações.

Exportando configurações

Para exportar as configurações para um arquivo de configuração:

1. Na árvore do Console do Aplicativo, execute uma das seguintes ações:

   - No menu de contexto do node **Kaspersky Embedded Systems Security for Windows**, selecione **Exportar configurações** para exportar todas as configurações do Kaspersky Embedded Systems Security for Windows.
   - No menu de contexto de uma tarefa específica, selecione **Exportar configurações** para exportar as configurações de um componente funcional individual do aplicativo.
   - Para exportar as configurações da Zona Confiável:

     a. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Kaspersky Embedded Systems Security for Windows**.

     b. Selecione **Configurar a Zona Confiável**.

     A janela **Zona Confiável** é exibida.

     c. Clique no botão **Exportar**.

     O Assistente de exportação de configurações é aberto.

2. Siga as instruções no **Assistente de Exportação de Configurações**: especifique o nome e caminho do arquivo de configuração que deseja usar para salvar as configurações.

   É possível utilizar as variáveis de ambiente do sistema ao especificar o caminho, mas não as variáveis de ambiente do usuário.

   Se uma política do Kaspersky Security Center estiver ativa no momento da exportação, o aplicativo exportará as configurações usados por essa política.

3. Clique no botão **Exportação de configurações do aplicativo concluída** na janela **Fechar**.

O Assistente de exportação de configurações fecha e salva as configurações exportadas.

Importando configurações

Para importar as configurações de um arquivo de configuração salvo:

1. Na árvore do Console do Aplicativo, execute uma das seguintes ações:

   - No menu de contexto do node **Kaspersky Embedded Systems Security for Windows**, selecione **Importar configurações** para importar todas as configurações do Kaspersky Embedded Systems Security for Windows.

- No menu de contexto de uma tarefa específica, selecione **Importar configurações** para importar as configurações de um componente funcional individual do aplicativo.
- Para importar as configurações da Zona Confiável:
  a. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Kaspersky Embedded Systems Security for Windows**.
  b. Selecione **Configurar a Zona Confiável**.
     A janela **Zona Confiável** é exibida.
  c. Clique no botão **Importar**.
     O Assistente de importação de configurações é aberto.

2. Siga as instruções do **Assistente de Importação de Configurações**: especifique o arquivo de configuração com as configurações que deseja importar.

   Depois de importar as configurações gerais do Kaspersky Embedded Systems Security for Windows ou de seus componentes funcionais para o dispositivo protegido, não será possível reverter para as configurações anteriores.

3. Clique no botão **Importação de configurações do aplicativo concluída** na janela **Fechar**.
   O Assistente de importação de configurações fecha e salva as configurações importadas.
4. Na barra de ferramentas do Console do Aplicativo, clique no botão **Atualizar**.

A janela do Console do Aplicativo exibe as configurações importadas.

O Kaspersky Embedded Systems Security for Windows não importa senhas (credenciais das contas para iniciar tarefas ou estabelecer a conexão com o servidor proxy) de um arquivo em outro dispositivo protegido ou no mesmo dispositivo protegido depois que o Kaspersky Embedded Systems Security for Windows tiver sido reinstalado ou atualizado nele. Após a conclusão da importação, as senhas deverão ser inseridas manualmente.

Usando os modelos de configurações de segurança

Esta seção contém informações sobre a utilização de modelos de configurações de segurança em tarefas de proteção e verificação do Kaspersky Embedded Systems Security for Windows.

Sobre os modelos de configurações de segurança

É possível definir manualmente as configurações de segurança de um nó na árvore ou em uma lista dos recursos de arquivos do dispositivo protegido e salvar os valores das configurações como um modelo. O modelo pode então ser utilizado para especificar as configurações de segurança de outros nodes nas tarefas de proteção e de verificação do Kaspersky Embedded Systems Security for Windows.

Os modelos podem ser utilizados para definir as configurações de segurança das seguintes tarefas do Kaspersky Embedded Systems Security for Windows:

- Proteção de Arquivos em Tempo Real
- Verificação na Inicialização do Sistema Operacional
- Verificação de Áreas Críticas
- Tarefas de Verificação por Demanda

As configurações de segurança de um modelo aplicadas a um node principal na árvore de recursos de arquivos do dispositivo protegido são aplicadas a todos os nodes secundários. O modelo do node principal não é aplicado aos nodes secundários nos seguintes casos:

- Caso as configurações de segurança dos nodes secundários tenham sido especificadas separadamente.
- Se os nodes secundários forem virtuais. Nesse caso, é necessário aplicar o modelo a cada nó virtual separadamente.

Criação de um modelo de configurações de segurança

Para salvar manualmente as configurações de segurança de um nó em um modelo:

1. Na árvore do Console do Aplicativo, selecione a tarefa para a qual deseja criar um modelo de configurações de segurança.
2. No painel de detalhes da tarefa selecionada, clique no link **Configurar o escopo da proteção** ou **Configurar o escopo da verificação**.
3. Na árvore ou lista de recursos de arquivos de rede do dispositivo protegido, selecione o modelo que deseja exibir.
4. Na guia **Nível de segurança**, clique no botão **Salvar como modelo**.

   A janela **Propriedades do modelo** é exibida.
5. No campo **Nome modelo**, digite o nome do modelo.
6. No campo **Descrição**, insira as informações adicionais do modelo.
7. Clique no botão **OK**.

O modelo de configurações de segurança é salvo.

Exibindo configurações de segurança em um modelo

Para visualizar as configurações de segurança em um modelo criado:

1. Na árvore do Console do Aplicativo, selecione a tarefa com o modelo de configurações de segurança que deseja visualizar.
2. No menu de contexto da tarefa selecionada, selecione **Modelos de configurações**.

A janela **Modelos** é exibida.

3. Na lista de modelos, selecione o modelo que deseja visualizar.

4. Clique no botão **Exibir**.

A janela **<Nome do modelo>** é exibida. A guia **Geral** exibe o nome do modelo e as informações adicionais sobre ele. A guia **Opções** lista as configurações de segurança salvas no modelo.

Aplicação de um modelo de configurações de segurança

Para aplicar configurações de segurança de um modelo a um nó selecionado:

1. Na árvore do Console do Aplicativo, selecione a tarefa à qual deseja aplicar um modelo de configurações de segurança.

2. No painel de detalhes da tarefa selecionada, clique no link **Configurar o escopo da proteção** ou **Configurar o escopo da verificação**.

3. Na árvore ou lista de recursos de arquivos de rede do dispositivo protegido, abra o menu de contexto do nó ou item ao qual deseja aplicar o modelo.

4. Selecione **Aplicar modelo → <Nome do modelo>**.

5. Clique no botão **Salvar**.

Isso aplicará o modelo de configurações de segurança ao node selecionado na árvore de recursos de arquivos do dispositivo protegido. O valor na guia **Nível de segurança** para o node selecionado muda para **Personalizado**.

Caso as configurações de segurança de um modelo sejam aplicadas a um node principal na árvore de recursos de arquivos do dispositivo protegido, essas configurações também serão aplicadas a todos os nodes secundários.

É possível configurar a proteção ou o escopo da verificação de nós filhos na árvore de recursos de arquivo do dispositivo protegido separadamente. Nesse caso, as configurações de segurança do modelo aplicado ao node principal não são aplicadas automaticamente aos nodes secundários.

Para aplicar configurações de segurança de um modelo a todos os nodes selecionados:

1. Na árvore do Console do Aplicativo, selecione a tarefa à qual deseja aplicar um modelo de configurações de segurança.

2. No painel de detalhes da tarefa selecionada, clique no link **Configurar o escopo da proteção** ou **Configurar o escopo da verificação**.

3. Na árvore ou lista de recursos de arquivos de rede do dispositivo protegido, selecione um node principal para aplicar o modelo ao node selecionado e aos nodes secundários.

4. No menu de contexto, selecione **Aplicar modelo → <Nome do modelo>**.

5. Clique no botão **Salvar**.

O modelo de configurações de segurança é aplicado ao node principal e a todos os nodes secundários na árvore de recursos de arquivos do dispositivo protegido. O valor na guia **Nível de segurança** para o node selecionado muda para **Personalizado**.

Exclusão de um modelo de configurações de segurança

Para excluir um modelo de configurações de segurança:

1. Na árvore do Console do Aplicativo, selecione a tarefa com o modelo de configurações de segurança que deseja excluir.
2. No menu de contexto da tarefa selecionada, selecione **Modelos de configurações**.

   A janela **Modelos** é exibida.

   No painel de resultados do node principal **Verificação por demanda**, é possível visualizar os modelos de configurações para tarefas de Verificação por Demanda.
3. Na lista de modelos, selecione o modelo que deseja excluir.
4. Clique no botão **Remover**.

   Uma janela é exibida para confirmar a exclusão.
5. Na janela exibida, clique em **Sim**.

O modelo selecionado é excluído.

É possível aplicar o modelo de configurações de segurança para proteger ou verificar os nodes na árvore de recursos de arquivos do dispositivo protegido. Nesse caso, as configurações de segurança para esses nós não são alteradas após a exclusão do modelo.

Visualizando o status de proteção e as informações do Kaspersky Embedded Systems Security for Windows

Para visualizar informações sobre o status de proteção do dispositivo do Kaspersky Embedded Systems Security for Windows,

selecione o node **Kaspersky Embedded Systems Security for Windows** na árvore do Console do Aplicativo.

Por padrão, as informações no painel de detalhes do Console do Aplicativo são atualizadas automaticamente:

- A cada 10 segundos, no caso de uma conexão local.
- A cada 15 segundos, no caso de uma conexão remota.

É possível atualizar as informações manualmente.

*Para atualizar as informações no node **Kaspersky Embedded Systems Security for Windows** manualmente,*

selecione o comando **Atualizar** no menu de contexto do node do **Kaspersky Embedded Systems Security for Windows**.

As seguintes informações do aplicativo são exibidas no painel de detalhes do Console do Aplicativo:

- Status de uso da Kaspersky Security Network.
- Status de proteção do dispositivo.
- Informações sobre as atualizações do banco de dados e do módulo do aplicativo.
- Dados de diagnóstico reais.
- Dados sobre tarefas de controle de dispositivos protegidos.
- Informações da licença.
- Status da integração com o Kaspersky Security Center: os detalhes do servidor com o Kaspersky Security Center instalado e com o qual o aplicativo está conectado; as informações sobre as tarefas do aplicativo controladas pela política ativa.

O código de cores é usado para exibir o status de proteção:

- *Verde*. A tarefa está sendo executada de acordo com as configurações definidas. A proteção está ativa.
- *Amarelo*. A tarefa não foi iniciada, está em pausa ou foi interrompida. Podem ocorrer ameaças de segurança. Aconselha-se a configuração e inicialização da tarefa.
- *Vermelho*. Tarefa concluída com um erro ou uma ameaça de segurança foi detectada enquanto a tarefa estava sendo executada. Aconselha-se iniciar a tarefa ou tomar medidas para eliminar a ameaça de segurança detectada.

Alguns detalhes neste bloco (por exemplo, nomes de tarefa ou o número de ameaças detectadas) são links que, quando clicados, o levam ao node da tarefa relevante ou abrem o log de tarefas.

A seção **Uso da Kaspersky Security Network** exibe o status atual da tarefa, por exemplo, *Executando*, *Interrompida* ou *Nunca foi executada*. O indicador pode ter os seguintes valores:

- A cor verde indica que a tarefa de Uso da KSN está em execução e as solicitações de arquivos para status estão sendo enviadas à KSN.
- A cor amarela indica que uma das Declarações foi aceita, mas a tarefa não está em execução; ou a tarefa está em execução, mas as solicitações de arquivos não estão sendo enviadas à KSN.

Proteção do computador

A seção **Proteção do Computador** (consulte a tabela abaixo) exibe informações sobre o status de proteção atual do dispositivo.

Informações sobre o status de proteção do dispositivo

Seção de Proteção	Informações
Indicador de status	A cor do painel com o nome da seção reflete o status das tarefas sendo executadas na seção. O indicador pode ter os seguintes valores:

de proteção do dispositivo	• Verde – Esta cor é exibida por padrão e significa que o componente de Proteção de Arquivos em Tempo Real está instalado e a tarefa está em execução. • Amarelo – O componente de Proteção de Arquivos em Tempo Real não está instalado, e a tarefa de Verificação de Áreas Críticas. não é executada há muito tempo. • Vermelho – A tarefa de Proteção de Arquivos em Tempo Real não está em execução.
Proteção de Arquivos em Tempo Real	**Status da tarefa** – status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Detectado** – Número de objetos detectados pelo Kaspersky Embedded Systems Security for Windows. Por exemplo, caso o Kaspersky Embedded Systems Security for Windows detecte o mesmo aplicativo malicioso em cinco arquivos, o valor desse campo aumentará em um. Se o número de aplicativos maliciosos detectados exceder 0, o valor será realçado em vermelho.
Verificação de Áreas Críticas	**Data da última verificação** – Data e hora da última Verificação de Áreas Críticas para quanto à existência de vírus e outras ameaças de segurança do computador. *Nunca foi executada* – um evento que ocorre quando a tarefa de Verificação de Áreas Críticas não foi executada nos últimos 30 dias ou mais (valor padrão). Você pode alterar o limite para gerar esse evento.
Prevenção de Exploits	**Status** – O status atual de técnicas de prevenção de exploits, por exemplo, *Aplicada* ou *Não aplicada*. **Modo de prevenção** – Um dos dois modos disponíveis, selecionado durante a configuração da proteção da memória do processo: **Encerrar no exploit** ou **Somente estatísticas**. **Processos protegidos** – O número total de processos adicionados ao escopo da proteção e tratado conforme o modo selecionado.
Objetos do backup	*Limite de espaço disponível no Backup excedido* – Este evento ocorre quando o limite de espaço disponível no Backup está se aproximando do limite especificado. O Kaspersky Embedded Systems Security for Windows continua a mover objetos para o Backup. Nesse caso, o valor no campo **Espaço usado** é realçado em amarelo. *Tamanho máximo do backup excedido*: esse evento ocorre quando o tamanho do backup alcança o limite especificado. O Kaspersky Embedded Systems Security for Windows continua a mover objetos para o Backup. Nesse caso, o valor no campo **Espaço usado** é realçado em vermelho. **Objetos do backup** - o número de objetos atualmente no Backup. **Espaço usado**: volume de espaço usado no Backup.

Atualização

A seção **Atualização** (consulte a tabela abaixo) exibe informações sobre o nível de atualização dos bancos de dados e dos módulos do aplicativo.

Informações sobre o status dos bancos de dados e módulos do Kaspersky Embedded Systems Security for Windows

Seção Atualização	Informações
Indicador de status dos bancos de dados e módulos de software	A cor do painel com o nome da seção reflete o status dos bancos de dados e módulos do aplicativo. O indicador pode ter os seguintes valores: • Verde – Esta cor é exibida por padrão e significa que os bancos de dados do aplicativo estão atualizados e que a última tarefa de atualização do banco de dados foi concluída com sucesso.

	• Amarelo – Os bancos de dados estão desatualizados ou a última tarefa de atualização do banco de dados apresentou falha. • Vermelho – O evento *O banco de dados do aplicativo está muito desatualizado* ou *O Banco de dados do aplicativo está corrompido* ocorreu.
Atualização do Banco de Dados e **Atualização dos Módulos de Software**	**Status do banco de dados**: uma avaliação do status de atualização do banco de dados. A opção pode ter os seguintes valores: • **O banco de dados do aplicativo está atualizado** – os bancos de dados do aplicativo foram atualizados há no máximo 7 dias (padrão). • **O banco de dados do aplicativo está desatualizado** – os bancos de dados do aplicativo foram atualizados entre 7 e 14 dias atrás (padrão). • **O banco de dados do aplicativo está muito desatualizado** – Os bancos de dados do aplicativo foram atualizados há mais de 14 dias (padrão). Você pode alterar os limites para gerar os eventos *O banco de dados do aplicativo está atualizado* e *O banco de dados do aplicativo está muito desatualizado*. **Data da versão do banco de dados do aplicativo** – a data e hora do lançamento da última atualização dos bancos de dados. A data e hora são especificadas em formato UTC. **Status da última tarefa de Atualização do banco de dados concluída** – data e hora da última atualização do banco de dados. A data e hora são especificadas de acordo com a hora local do dispositivo protegido. O campo fica vermelho caso ocorra o evento de *Falhou*. **Número de atualizações de módulo disponíveis** – o número de atualizações do módulo do Kaspersky Embedded Systems Security for Windows disponíveis para ser baixadas e instaladas. **Número de atualizações de módulo instaladas** – o número de atualizações do módulo do Kaspersky Embedded Systems Security for Windows instaladas.

Controle

A seção **Controle** (consulte a tabela abaixo) exibe informações sobre as tarefas de Controle de Inicialização de Aplicativos, Controle de Dispositivos e Gerenciamento de Firewall.

Informações sobre o status do controle de dispositivos protegidos

Seção Controle	Informações
Indicador de status para controle de dispositivos protegidos	A cor do painel com o nome da seção reflete o status das tarefas sendo executadas na seção. O indicador pode ter os seguintes valores: • Verde – Esta cor é exibida por padrão e significa que o componente Controle de Inicialização de Aplicativos está instalado e a tarefa está em execução no modo **Ativa**. • Amarelo – O Controle de Inicialização de Aplicativos está em execução no modo **Somente estatísticas**. • Vermelho – a tarefa de Controle de Inicialização de Aplicativos não está em execução ou apresentou falha.

Controle de Inicialização de Aplicativos	**Status da tarefa** – status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Modo de operação** – um dos dois modos disponíveis para a tarefa de Controle de Inicialização de Aplicativos: **Ativa** ou **Somente estatísticas**. **Inicializações de aplicativos negadas** – o número de tentativas de iniciar aplicativos bloqueadas pelo Kaspersky Embedded Systems Security for Windows durante a tarefa de Controle de Inicialização de Aplicativos. Se o número de inicializações de aplicativo bloqueadas exceder 0, o campo ficará vermelho. **Tempo médio de processamento (ms)** – Tempo que levou para o Kaspersky Embedded Systems Security for Windows processar uma tentativa de iniciar aplicativos no dispositivo protegido.
Controle de dispositivos	**Status da tarefa** – status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Modo de operação** - um dos dois modos disponíveis para a tarefa de Controle de Dispositivos: **Ativa** ou **Somente estatísticas**. **Dispositivos bloqueados** – Número de tentativas para conectar um dispositivo externo bloqueado pelo Kaspersky Embedded Systems Security for Windows durante a tarefa de Controle de Dispositivos. Se o número de dispositivos externos bloqueados exceder 0, o valor do campo ficará vermelho.
Gerenciamento de firewall	**Status da tarefa** – status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Tentativas de conexões bloqueadas** – o número de conexões a um dispositivo protegido bloqueadas pelas regras do firewall especificadas.

Diagnósticos

A seção **Diagnósticos** (consulte a tabela abaixo) exibe informações sobre as tarefas de Monitor de Integridade de Arquivos e Inspeção do Log.

Informação sobre o status de Inspeção do sistema

Seção Diagnósticos	Informações
Indicador de status de diagnóstico	A cor do painel com o nome da seção reflete o status das tarefas sendo executadas na seção. O indicador pode ter os seguintes valores: • Verde – Esta cor é exibida por padrão e significa que um ou ambos os componentes de inspeção de sistema estão instalados e as tarefas estão em execução. • Amarelo – ambos os componentes estão instalados, mas uma das tarefas de inspeção do sistema não está em execução; ocorreu o evento *Não está em execução*. • Vermelho – uma das tarefas falhou.
Monitor de Integridade de Arquivos	**Status da tarefa** – status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Operações de arquivos não sancionadas** – o número de alterações em arquivos dentro do escopo de monitoramento. Essas modificações podem indicar que a segurança de um dispositivo protegido foi violada.
Inspeção do Log	**Status da tarefa** – status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Violações das regras configuradas** – Número de violações registradas com base em dados do Log de Eventos do Windows. Este número é determinado com base nas regras de tarefa especificadas ou usando o analisador heurístico.

As informações sobre o licenciamento do Kaspersky Embedded Systems Security for Windows são exibidas na linha no canto inferior esquerdo no painel de detalhes do nó do **Kaspersky Embedded Systems Security for Windows**.

É possível configurar as propriedades do Kaspersky Embedded Systems Security for Windows seguindo o link **Propriedades do aplicativo**.

É possível se conectar em um dispositivo protegido diferente acessando o link **Conectar a outro computador**.

Trabalhando com o plug-in da Web a partir do Web Console e Cloud Console

Esta seção fornece informações sobre o Plug-in de Administração do Kaspersky Embedded Systems Security for Windows e descreve como gerenciar o aplicativo instalado em um dispositivo protegido ou em um grupo de dispositivos protegidos.

Gerenciamento do Kaspersky Embedded Systems Security for Windows a partir do Web Console e Cloud Console

É possível gerenciar de forma centralizada vários dispositivos protegidos que tenham o Kaspersky Embedded Systems Security for Windows instalado e incluído em um grupo de administração usando o Plug-in da Web do Kaspersky Embedded Systems Security for Windows. O Kaspersky Security Center Web Console e o Kaspersky Security Center Cloud Console também permitem definir as configurações de cada dispositivo protegido incluído em um grupo de administração separadamente.

Um grupo de administração é criado manualmente no Kaspersky Security Center Web Console. O grupo inclui vários dispositivos com o Kaspersky Embedded Systems Security for Windows instalado para os quais se 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*.

Não será possível configurar o aplicativo para um único dispositivo protegido caso a operação do Kaspersky Embedded Systems Security for Windows no dispositivo protegido seja controlada por uma política ativa do Kaspersky Security Center.

O Kaspersky Embedded Systems Security for Windows pode ser gerenciado do Kaspersky Security Center Web Console 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 dispositivos. As configurações de tarefa especificadas na política ativa têm prioridade sobre as configurações de tarefa definidas localmente no Console do Aplicativo ou remotamente na janela de propriedades do dispositivo no Kaspersky Security Center Web Console. As políticas podem ser usadas para definir configurações gerais do aplicativo, configurações para tarefas de proteção do computador em tempo real, tarefas de controle de atividade em dispositivos e configurações para iniciar as tarefas locais do sistema em um agendamento.

- **Usando tarefas de grupo do Kaspersky Security Center**. Com as tarefas de grupo do Kaspersky Security Center, é possível definir remotamente configurações comuns de tarefas com um período de validade para um grupo de dispositivos. 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 do Gerador de Regras de Controle de Inicialização de Aplicativos.

- **Usando tarefas para um grupo de dispositivos**. As tarefas para um conjunto de dispositivos permitem definir remotamente as configurações comuns de tarefa com um período de execução limitado para os dispositivos protegidos que não pertencem a nenhum dos grupos de administração.

- **Usando a janela de propriedades de um único dispositivo**. Na janela de propriedades do dispositivo, é possível definir remotamente as configurações de tarefa de um único dispositivo protegido incluído no grupo de administração. É possível definir tanto as configurações gerais do aplicativo como as configurações de todas as tarefas do Kaspersky Embedded Systems Security for Windows caso o dispositivo protegido selecionado não seja controlado por uma política ativa do Kaspersky Security Center.

O Kaspersky Security Center Web Console e o Kaspersky Security Center Cloud Console permitem definir as configurações e recursos avançados do aplicativo e trabalhar com logs e notificações. É possível definir essas configurações para um grupo de dispositivos protegidos e para um dispositivo protegido individual.

Limitações do Plug-in da Web

O plug-in da Web do Kaspersky Embedded Systems Security for Windows tem as seguintes limitações em comparação ao Plug-in de Administração do Kaspersky Embedded Systems Security for Windows:

- Para adicionar usuários ou grupos de usuários, é necessário especificar as sequências do descritor de segurança utilizando a linguagem de definição do descritor de segurança (SDDL).
- O nível de segurança predefinido não pode ser alterado para a tarefa de Proteção de arquivos em tempo real.
- As regras da tarefa de Controle de Inicialização de Aplicativos não podem ser criadas utilizando certificados digitais ou eventos do Kaspersky Security Center.
- As regras da tarefa de Controle de dispositivos não podem ser geradas de acordo com os dispositivos conectados ou com os dados do sistema.

Gerenciamento das configurações do aplicativo

Esta seção contém informações sobre como definir as configurações gerais do Kaspersky Embedded Systems Security for Windows no Kaspersky Security Center Web Console.

Definição das configurações gerais do aplicativo no plug-in da Web

É possível definir as configurações gerais do Kaspersky Embedded Systems Security for Windows no plug-in da Web para um grupo de dispositivos protegidos ou um dispositivo protegido.

Definição das configurações de escalabilidade, interface e verificação no plug-in da Web

Para configurar configurações de escalabilidade e a interface do aplicativo:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos → Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Configurações do aplicativo**.
5. Clique no botão **Configurações** na subseção **Configurações de escalabilidade, interface e verificação**.
6. Defina as configurações descritas na tabela a seguir.

Configuração	Descrição
Detectar automaticamente as configurações de escalabilidade	O Kaspersky Embedded Systems Security for Windows controla automaticamente o número de processos utilizados. Este é o valor padrão.
Definir manualmente o número de processos em andamento	O Kaspersky Embedded Systems Security for Windows controla o número de processos de trabalho ativos de acordo com os valores especificados.
Número de processos para a Proteção em Tempo Real	O número máximo de processos usados pelos componentes da tarefa de Proteção do Computador em Tempo Real. O campo de inserção de dados está disponível se a opção **Definir manualmente o número de processos em andamento** estiver selecionada.
Número de processos de tarefas de verificação por demanda em segundo plano	Número máximo de processos utilizados pelo componente de Verificação por Demanda ao executar suas tarefas em segundo plano. O campo de inserção de dados está disponível se a opção **Definir manualmente o número de processos em andamento** estiver selecionada.
Exibir o ícone da Bandeja do Sistema na barra de tarefas	Configurar se o ícone da bandeja do sistema será exibido na área de notificação.
Restaurar os atributos do arquivo após a verificação	Quando o Kaspersky Embedded Systems Security for Windows executa as tarefas de Verificação por Demanda e Proteção de Arquivos em Tempo Real, a hora em que cada arquivo verificado foi acessado pela última vez é atualizada. Após a verificação, o Kaspersky Embedded Systems Security for Windows redefine a hora em que o arquivo foi acessado pela última vez para o valor inicial. Esse comportamento pode afetar o trabalho dos sistemas de backup ao causar a criação de cópias de backup para arquivos não alterados. Isso também pode causar detecções falsas em aplicativos de rastreamento de alterações de arquivos. Por padrão, essa função está ativada.
Limitar a utilização da CPU para threads de verificação	O Kaspersky Embedded Systems Security for Windows limita o uso da CPU do dispositivo protegido durante as tarefas de Verificação por Demanda ao valor especificado no campo **Limite superior (porcento)**. A ativação dessa opção pode afetar negativamente o desempenho do Kaspersky Embedded Systems Security for Windows. Por padrão, essa opção está desativada.
Limite superior (em porcentagem)	Valor máximo permitido de utilização da CPU pelo Kaspersky Embedded Systems Security for Windows. O campo de entrada está disponível caso a opção **Limitar a utilização da CPU para threads de verificação** esteja selecionada.
Pasta para os arquivos temporários	Pasta na qual o Kaspersky Embedded Systems Security for Windows precisa descompactar os arquivos compactados durante a verificação.

criados durante a verificação	Por padrão, a pasta C:\Windows\Temp é utilizada.
Configurações do sistema HSM	Selecionar a opção para acessar o armazenamento hierárquico.

Definição das configurações de segurança no plug-in da Web

Para definir as configurações de segurança manualmente, siga as etapas a seguir:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Configurações do aplicativo**.
5. Clique no botão **Configurações** na subseção **Segurança e confiabilidade**.
6. Defina as configurações descritas na tabela a seguir.

Configurações de segurança

Configuração	Descrição
Proteger os processos de aplicativos contra ameaças externas	Caso a função **Proteger os processos de aplicativos contra ameaças externas** esteja ativada, o aplicativo protege os processos contra a injeção de códigos ou o acesso a dados de processos. Ao ativar ou desativar essa função, não há necessidade de reiniciar os serviços do aplicativo para que as alterações sejam aplicadas. Essa função é ativada por padrão.
Executar recuperação da tarefa	Esta caixa de seleção ativa ou desativa a recuperação do Kaspersky Embedded Systems Security for Windows quando houver um erro ou o aplicativo for encerrado. Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows recuperará automaticamente as tarefas do Kaspersky Embedded Systems Security for Windows quando houver um erro ou o aplicativo for encerrado. Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows não recuperará automaticamente as tarefas do Kaspersky Embedded Systems Security for Windows quando houver um erro ou o aplicativo for encerrado. A caixa de seleção é marcada por padrão.
Recuperar tarefas de Verificação por Demanda não mais que (vezes) na faixa de 1 - 10 tentativas	O número de tentativas de recuperação de uma tarefa de Verificação por Demanda após o Kaspersky Embedded Systems Security for Windows retornar um erro. O campo de entrada estará disponível se a caixa de seleção **Executar recuperação da tarefa** estiver marcada.
Não iniciar tarefas de verificação agendadas	Esta caixa de seleção ativa ou desativa a inicialização de uma tarefa de

	verificação programada após o dispositivo protegido mudar para uma fonte de energia UPS até que o fornecimento de energia padrão seja restaurado. Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows não executará as tarefas de verificação programadas após o dispositivo protegido mudar para uma fonte UPS até que o fornecimento de energia padrão seja restaurado. Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows executará as tarefas de verificação independentemente do fornecimento de energia. A caixa de seleção é marcada por padrão.
Interromper tarefas de verificação atuais	A caixa de seleção ativa ou desativa a execução das tarefas de verificação após o dispositivo protegido mudar para uma fonte UPS. Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows pausará as tarefas de verificação em execução após o dispositivo protegido mudar para uma fonte UPS. Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows continuará as tarefas de verificação em execução após o dispositivo protegido mudar para uma fonte UPS. A caixa de seleção é marcada por padrão.
Aplicar proteção de senha	Defina uma senha para proteger o acesso às funções do Kaspersky Embedded Systems Security for Windows.

Definição das configurações de conexão no plug-in da Web

As configurações de conexão definidas são usadas para conectar o Kaspersky Embedded Systems Security for Windows 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. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Configurações do aplicativo**.
5. Clique no botão **Configurações** na subseção **Configurações de escalabilidade, interface e verificação**.
6. Defina as configurações descritas na tabela a seguir.

Configurações de conexão

Configuração	Descrição
Não usar o servidor proxy	Se esta opção estiver selecionada, o Kaspersky Embedded Systems Security for Windows conecta-se a serviços da KSN diretamente, sem usar nenhum servidor proxy.
Usar configurações de servidor proxy especificadas	Se esta opção estiver selecionada, o Kaspersky Embedded Systems Security for Windows se conectará a KSN usando configurações de servidor proxy especificadas manualmente.

Não usar o servidor proxy para endereços locais	Essa caixa ativa ou desativa a utilização de um servidor proxy ao acessar os dispositivos localizados na mesma rede do dispositivo protegido com o Kaspersky Embedded Systems Security for Windows instalado. Se esta caixa de seleção estiver marcada, os dispositivos serão acessados diretamente na rede que hospeda o dispositivo protegido com o Kaspersky Embedded Systems Security for Windows instalado. Nenhum servidor proxy é usado. Se a caixa estiver desmarcada, o servidor proxy será usado para se conectar a dispositivos locais. A caixa de seleção é marcada por padrão.
Configurações de autenticação do servidor proxy	Especificar as configurações de autenticação
Não usar autenticação	A autenticação não é realizada. O 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 é realizada com um nome de usuário e senha usando o protocolo de autenticação de rede NTLM desenvolvido pela Microsoft.
Aplicar nome de usuário e senha	A autenticação é realizada usando o nome de usuário e a senha.

Configuração da inicialização programada de tarefas locais do sistema

É possível utilizar as políticas para permitir ou bloquear o início das tarefas locais do sistema de Verificação por Demanda e de Atualização. Isso é feito de acordo com a programação configurada localmente em cada dispositivo protegido 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 dispositivo protegido 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 se atualizações ou verificações por demanda estiverem sendo administradas por tarefas de grupo do Kaspersky Security Center.

Caso você não use as tarefas de atualização de grupo e Verificação por Demanda, permita que as tarefas locais do sistema sejam inicializadas na política: o Kaspersky Embedded Systems Security for Windows executará atualizações de banco de dados do aplicativo e de módulos, e iniciará todas as tarefas locais do sistema de Verificação por Demanda de acordo com a programação padrão.

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

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

Caso o dispositivo protegido seja excluído do grupo de administração, a programação de tarefas locais do sistema será ativada automaticamente.

Para permitir ou bloquear a inicialização programada de tarefas locais do sistema do Kaspersky Embedded Systems Security for Windows em uma política:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Configurações do aplicativo**.
5. Clique no botão **Configurações** na subseção **Executar as tarefas do sistema local**.
6. Defina as configurações descritas na tabela a seguir.

Configurações de inicialização programada de tarefas locais do sistema

Configuração	Descrição
Permitir inicialização de tarefas de verificação por demanda	Marque ou desmarque a caixa de seleção para permitir ou proibir o início programado de tarefas de Verificação por Demanda.
Permitir tarefas de atualização e inicialização da tarefa de Cópia de atualização	Marque ou desmarque a caixa de seleção para permitir ou proibir o início programado de tarefas de atualização e da tarefa Copiar atualizações.

Definição das configurações de Quarentena e Backup no Plug-in da Web

Para definir as configurações gerais da Quarentena e do Backup no Kaspersky Security Center:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Suplementar**.
5. Clique no botão **Configurações** na subseção **Armazenamentos**.

6. Defina as configurações descritas na tabela a seguir.

Configurações da Quarentena e do Backup

Configuração	Descrição
Pasta de backup	Especificar a pasta de Backup.
Tamanho máximo do backup (MB)	Definir o tamanho máximo do Backup.
Valor limite de espaço disponível (MB)	Especificar o valor mínimo de espaço livre na pasta de Backup.
Pasta destino para a restauração de objetos	Especificar uma pasta para os objetos restaurados.
Pasta da Quarentena	Especificar a pasta de Backup.
Tamanho máximo da Quarentena (MB)	Definir o tamanho máximo do Backup.
Valor limite de espaço disponível (MB)	Especificar o valor mínimo de espaço livre na pasta de Backup.
Pasta destino para a restauração de objetos	Especificar uma pasta para os objetos restaurados.
Termo de bloqueio da sessão de rede	Especifique o número de dias, horas e minutos após os quais os hosts bloqueados recuperam o acesso aos recursos de arquivos de rede.

Criação e configuração de políticas

Esta seção fornece informações sobre a utilização de políticas do Kaspersky Security Center para gerenciar o Kaspersky Embedded Systems Security for Windows em vários dispositivos protegidos.

As políticas globais do Kaspersky Security Center podem ser criadas para gerenciar a proteção em vários dispositivos onde o Kaspersky Embedded Systems Security for Windows está instalado.

Uma política impõe as configurações, funções e tarefas do Kaspersky Embedded Systems Security for Windows especificadas nela a todos os dispositivos protegidos para 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 for Windows. Essas informações podem ser visualizadas no Console do Aplicativo, no node **Log de auditoria do sistema**.

O Kaspersky Security Center oferece uma maneira para aplicar políticas em computadores locais: *Proibir a alteração das configurações*. Após a aplicação de uma política, o Kaspersky Embedded Systems Security for Windows utiliza as configurações para as quais o ícone foi selecionado nas propriedades da política em dispositivos protegidos. Nesse caso, as configurações selecionadas são utilizadas em vez das configurações em vigor antes da aplicação da política. O Kaspersky Embedded Systems Security for Windows não aplica as configurações de política ativa para as quais o ícone está 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 as alterações no Kaspersky Security Center para um dispositivo protegido individual na janela **Propriedades: <Nome do dispositivo protegido>**.

As configurações especificadas e enviadas para o dispositivo protegido usando uma política ativa são salvas nas configurações da tarefa local após a política ativa ser desativada.

Caso uma política defina as configurações de qualquer tarefa de Proteção do Computador em Tempo Real em execução, as configurações definidas pela política serão alteradas imediatamente após a política ser aplicada. Se a tarefa não estiver sendo executada, as configurações serão aplicadas quando ela for iniciada.

Criando uma política

Para criar uma política:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no botão **Adicionar**.
3. A janela **Nova política** é exibida.
4. Na seção **Selecionar aplicativo**, selecione o Kaspersky Embedded Systems Security for Windows e clique em **Próximo**.
5. Na guia **Geral**, você pode executar as seguintes ações:
   - Altere o nome da política.

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

   - Selecionar o status da política:
     - **Ativa**. Após a próxima sincronização, a política será usada como a política ativa no computador.
     - **Inativa**. Política de Backup. Se necessário, uma política inativa poderá ser alterada para o status ativo.
     - **Ausente**. A política é ativada quando um computador deixa o perímetro da rede da organização.
   - Defina a herança das configurações:
     - **Herdar as configurações da política principal**. Se esse botão estiver ativado, os valores de configuração da política serão herdados da política de nível superior. As configurações da política não podem ser editadas se estiver definido para a política principal.
     - **Forçar a herança das configurações nas políticas secundárias**. Se o botão estiver ativado, os valores das configurações da política serão propagados para as políticas secundárias. Nas configurações da política secundária, a caixa de seleção **Herdar configurações da política principal** é marcada automaticamente. As configurações da política secundária são herdadas da política principal, exceto as configurações marcadas com . As configurações da política secundária não podem ser editadas se estiver definido para a política principal.

6. Na guia **Configurações do aplicativo**, defina as configurações da política, conforme necessário.

7. Clique no botão **Salvar**.

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

Após a criação de uma nova política, um conjunto de regras de permissão é criado para impedir que os aplicativos sejam bloqueados e garantir a operação ininterrupta. É possível exibir as estatísticas da tarefa no log de tarefas. Veja abaixo os detalhes e as limitações.

Por padrão, o Kaspersky Embedded Systems Security for Windows cria um conjunto de regras para o tráfego de rede de entrada quando uma nova política é criada:

- Duas regras de permissão para o processo de compartilhamento da área de trabalho do Windows usando o Agente de Rede do Kaspersky Security Center, localizado nas pastas %Arquivos de Programas% e %Arquivos de Programas (x86)%. Estado: ativado. Endereços externos permitidos: todos. Protocolos: TCP e UPD (uma regra por protocolo).
- Duas regras de permissão para a porta local 15000. Estado: ativado. Endereços externos permitidos: todos. Protocolos: TCP e UPD (uma regra por protocolo).

Por padrão, o Kaspersky Embedded Systems Security for Windows cria um conjunto de regras para o tráfego de rede de saída quando uma nova política é criada:

- Duas regras de permissão para o serviço do Kaspersky Embedded Systems Security for Windows, localizado em %Arquivos de Programas% e %Arquivos de Programas (x86)%. Estado: ativado. Endereços externos permitidos: todos. Protocolos: TCP e UPD (uma regra por protocolo).
- Duas regras de permissão para o processo de trabalho do Kaspersky Embedded Systems Security for Windows, localizado nas pastas %Arquivos de programas% e %Arquivos de programas (x86)%. Estado: ativado. Endereços externos permitidos: todos. Protocolos: TCP e UPD (uma regra por protocolo).
- Duas regras de permissão para a porta local 13000. Estado: ativado. Endereços externos permitidos: todos. Protocolos: TCP e UPD (uma regra por protocolo).

Seções de configurações de política do Kaspersky Embedded Systems Security for Windows

Geral

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

- Indicar o status da política.
- Configurar as configurações de herança das políticas principais e secundárias.

Configuração de evento

Na seção **Configuração de evento**, é possível definir configurações para as seguintes categorias de evento:

- *Evento crítico*
- *Falha funcional*
- *Aviso*
- *Informação*

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 eventos registrados.
- Indicar o método de notificação para eventos registrados.

Configurações do aplicativo

Configurações da seção Configurações do aplicativo

Seção	Opções
Configurações de escalabilidade, interface e verificação	Na subseção **Configurações de escalabilidade, interface e verificação**, 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 e confiabilidade	Na subseção **Segurança e confiabilidade**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Definir as configurações de inicialização da tarefa. • Especificar como o aplicativo deve se comportar quando o dispositivo protegido estiver funcionando com a fonte de energia UPS. • Ativar ou desativar a proteção de senha das funções do aplicativo.
Conexões	Na subseção **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 as tarefas do sistema local	Na subseção **Executar as tarefas do sistema local**, é possível utilizar o botão **Configurações** para permitir ou bloquear a inicialização das seguintes tarefas locais do sistema de acordo com uma programação definida nos dispositivos protegidos: • Tarefa de Verificação por Demanda. • Tarefas de Atualização e Cópia de Atualizações.

Suplementar

Configurações da seção Suplementar

Seção	Opções
Zona Confiável	Na subseção **Configurações**, é possível clicar no botão **Zona Confiável** para definir as seguintes configurações da Zona Confiável: • 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	Na subseção **Verificação de unidades removíveis**, é possível usar o botão **Configurações** para definir configurações de verificação para drives removíveis.
Permissões de acesso do usuário para gerenciamento do aplicativo	Na subseção **Permissões de acesso do usuário para gerenciamento do aplicativo**, é possível configurar direitos de usuário e de grupos de usuários para gerenciar o Kaspersky Embedded Systems Security for Windows.
Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service	Na subseção **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service**, é possível configurar os direitos de usuário e de grupos de usuários para gerenciar o Kaspersky Security Service.
Armazenamentos	Na seção **Armazenamentos**, clique no botão **Configurações** para definir as seguintes configurações de Quarentena, Backup e Hosts Bloqueados: • Especificar o caminho da pasta onde deseja colocar objetos em Quarentena ou de Backup. • Configurar o tamanho máximo do Backup e Quarentena, alem de especificar o limite de espaço disponível. • Especificar o caminho da pasta onde deseja colocar os objetos restaurados da Quarentena ou Backup. • Configure a transmissão de informações sobre objetos em Quarentena e de Backup para o Servidor de Administração. • Configurar a forma como hosts longos são bloqueados.

Proteção do Computador em Tempo Real

Configurações da seção Proteção do Servidor em Tempo Real

Seção	Opções
Proteção de Arquivos em Tempo Real	Na subseção **Proteção de Arquivos em Tempo Real**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Indicar o modo de proteção. • Configurar o uso do Analisador Heurístico. • Configurar o aplicativo 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.
Prevenção de Exploits	Na subseção **Prevenção de Exploits**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Selecionar o modo de proteção da memória do processo. • Indicar ações para reduzir os riscos de exploit. • Adicionar e editar a lista de processos protegidos.

Controle de atividades locais

Configurações da seção Controle de Atividades Locais

Seção	Opções
Controle de Inicialização de Aplicativos	Na subseção **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 das regras de Controle de Inicialização de Aplicativos. • Configurar o uso da KSN. • Definir as configurações de inicialização da tarefa.
Controle de Dispositivos	Na subseção **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 atividades de rede

Configurações da seção Controle de Atividades de Rede

Seção	Opções
Gerenciamento de Firewall	Na subseção **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

Configurações da seção Inspeção do Sistema

Seção	Opções
Monitor de Integridade de Arquivos	Na subseção **Monitor de Integridade de Arquivos**, é possível configurar o controle sobre alterações em arquivos que podem significar uma violação de segurança em um dispositivo protegido.
Inspeção do Log	Na subseção **Inspeção do Log**, é possível configurar o monitoramento da integridade do dispositivo protegido de acordo com os resultados de uma análise do Log de Eventos do Windows.

Logs e notificações

Configurações da seção Logs e Notificações

Seção	Opções
Logs de tarefas	Na subseção **Logs 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 do Log de tarefas. • Especificar a integração SIEM com configurações do Kaspersky Security Center.
Notificações de eventos	Na subseção **Notificações de eventos**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Especificar as configurações de notificação de usuário para os eventos *Objeto detectado*, *Armazenamento em massa não confiável detectado e restringido* e *Host listado como não confiável*. • 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 subseção **Interação com o Servidor de Administração**, é possível clicar no botão **Configurações** para selecionar os tipos de objetos que o Kaspersky Embedded Systems Security for Windows 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.

Criando e configurando uma tarefa usando o Kaspersky Security Center

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

Sobre a criação de tarefas no plug-in da Web

É possível criar tarefas de grupo para grupos de administração e conjuntos de dispositivos protegidos. Os seguintes tipos de tarefas podem ser criados:

- 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
- Monitor de Comparação de Integridade de Arquivos
- 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 dispositivo protegido: na janela **Propriedades <Nome do dispositivo protegido>** na seção **Tarefas**.
- Para um grupo de administração: no painel de detalhes do node do grupo de dispositivos protegidos selecionado na guia **Tarefas**.
- Para um conjunto de dispositivos protegidos: no painel de detalhes do node **Seleções de dispositivos**.

Você pode usar as políticas para desativar as programações de tarefas locais do sistema para Atualização e Verificação por Demanda em todos os dispositivos 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 no plug-in da Web

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. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.

     b. Clique na guia **Grupos** para selecionar o grupo de administração ao qual o dispositivo protegido pertence.

     c. Clique no nome do dispositivo protegido.

     d. Na janela **<Nome do dispositivo>** que é exibida, selecione a guia **Tarefas**.

     e. Clique no botão **Adicionar**.

   - Para criar uma tarefa de grupo:

     a. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.

     b. Clique na guia **Grupos** para selecionar o grupo de administração para o qual deseja criar uma tarefa.

     c. Clique no botão **Adicionar**.

   - Para criar uma tarefa para um conjunto personalizado de dispositivos protegidos:

     a. Na janela principal do Web Console, selecione **Dispositivos** → **Seleções de dispositivos**.

     b. Marque a seleção para a qual você deseja criar uma tarefa.

     c. Clique no botão **Iniciar**.

     d. Na janela **Resultados da seleção**, selecione os dispositivos para os quais você deseja criar uma tarefa.

     e. Clique no botão **Nova tarefa**.

   A janela do assistente de tarefa é exibida.

2. Na lista suspensa **Aplicativo**, selecione **Kaspersky Embedded Systems Security for Windows**.

3. Na lista suspensa **Tipo de tarefa**, selecione o tipo de tarefa que deseja criar.

   Caso tenha selecionado qualquer tipo de tarefa, exceto Reversão da Atualização do Banco de Dados, Controle de Integridade de Aplicativos ou Ativação do Aplicativo, a janela Configurações será exibida.

4. Dependendo do tipo de tarefa selecionada, execute uma das seguintes ações:

   - Crie uma tarefa de Verificação por Demanda.

   - Para criar uma tarefa de atualização, defina as configurações da tarefa de acordo com suas necessidades:

     a. Selecione uma fonte de atualização na seção **Fonte de atualização do banco de dados**.

     b. Na janela **Configurações de conexão**, defina as configurações do servidor proxy.

- Após criar uma tarefa de Atualização dos Módulos de Software, defina as configurações necessárias de atualização dos módulos do aplicativo na janela **Atualização dos Módulos de Software**:

  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** for selecionado: um reinício do dispositivo protegido poderá ser necessário para aplicar os módulos de software instalados. Se desejar que o Kaspersky Embedded Systems Security for Windows reinicie o dispositivo protegido automaticamente após a conclusão da tarefa, selecione a caixa **Permitir reinício do sistema operacional**.

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

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

- Para criar a tarefa de Copiar Atualizações, especifique o conjunto de atualizações e a pasta de destino na janela **Copiar atualizações**.

- Para criar a tarefa de Ativação do Aplicativo:

  a. Na janela **Lista de chaves no armazenamento do Kaspersky Security Center**, especifique o arquivo de chave que deseja usar para ativar o aplicativo.

  b. Marque a caixa de seleção **Usar como chave adicional** se desejar criar uma tarefa para renovar a licença.

- Crie e configure a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos.

- Crie e configure a tarefa do Gerador de Regras de Controle de Dispositivos.

5. Clique no botão **Avançar**.

6. Se a tarefa estiver sendo criada para um conjunto de dispositivos protegidos, selecione a rede (ou grupo) de dispositivos protegidos na qual a tarefa será executada.

7. Clique no botão **Avançar**.

8. Caso queira definir as configurações da tarefa, na janela **Finalizar criação**, marque a caixa de seleção **Abrir detalhes da tarefa quando a criação for concluída**.

9. Clique no botão **Concluir**.

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

Configuração de tarefas de grupo no plug-in da Web

Para configurar a tarefa de grupo para múltiplos dispositivos protegidos:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Tarefas**.

2. Clique no nome da tarefa na lista de tarefas do Kaspersky Security Center.

   A janela **<Nome da tarefa>** é exibida.

3. 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 **Fontes de atualização**, defina as configurações de fonte de atualização e servidor proxy.

     b. Na seção **Otimização**, configure a otimização do subsistema de disco.

   - Para configurar a tarefa de Atualização dos Módulos de Software, na seção **Configurações avançadas** 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 da cópia de atualizações**.

   - Para configurar a tarefa de Ativação do Aplicativo, aplique o arquivo de chave que deseja usar para ativar o aplicativo. Selecione a caixa **Usar como chave adicional** caso deseje adicionar um código de ativação ou arquivo de chave para renovar a licença.

   - Para configurar a geração automática de regras de permissão para o Controle de Dispositivos, especifique as configurações que serão usadas para criar a lista de regras de permissão.

4. Configure a programação da tarefa na seção **Agendamento** (é possível configurar uma programação para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).

5. Na guia **Configurações**, na seção **Conta**, especifique a conta cujos direitos serão usados para executar a tarefa. Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

6. Clique no botão **Salvar**.

As recém-definidas configurações da tarefa de grupo são salvas.

Configuração da tarefa de Ativação do aplicativo no plug-in da Web

Para criar uma tarefa de Ativação do Aplicativo:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Tarefas**.

2. Clique no nome da tarefa na lista de tarefas do Kaspersky Security Center.

   A janela **<Nome da tarefa>** é exibida.

3. Na seção **Comum**, especifique o arquivo de chave que deseja usar para ativar o aplicativo. Marque a caixa de seleção **Usar como chave adicional** caso queira adicionar uma chave para renovar a licença.

4. Configure a programação da tarefa na seção **Agendamento**.

5. Na janela **<Nome da tarefa>**, clique em **OK**.

Configuração das tarefas de Atualização no plug-in da Web

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

1. Na janela principal do Web Console, selecione **Dispositivos** → **Tarefas**.

2. Clique no nome da tarefa na lista de tarefas do Kaspersky Security Center.

   A janela **<Nome da tarefa>** é exibida.

3. Na seção **Fontes de atualização**, defina as configurações de fonte de atualização:

   - Na seção **Fonte de atualização do banco de dados**, especifique o Servidor de Administração do Kaspersky Security Center ou os servidores de atualização da Kaspersky como fonte de atualização do aplicativo. Também é possível criar uma lista personalizada de fontes de atualização: adicionando servidores HTTP e FTP personalizados ou pastas de rede manualmente e definindo-os como fontes de atualização.

     É possível especificar o uso dos servidores de atualização da Kaspersky se servidores personalizados manualmente não estiverem disponíveis.

     > Para usar uma pasta compartilhada por SMB como uma fonte de atualização, é necessário especificar uma conta de usuário para iniciar uma tarefa.

     > Ao configurar uma tarefa de atualização por meio do Cloud Console, apenas as configurações **Pontos de distribuição** e **Servidores de atualização da Kaspersky** estão disponíveis para especificar a fonte de atualização.

   - Na seção **Configurações de conexão**, configure a utilização de um servidor proxy para conectar aos servidores de atualização da Kaspersky e outros servidores.

4. Na seção **Otimização** para a tarefa de Atualização do banco de dados, é possível configurar o recurso que reduz a carga de trabalho no subsistema de disco:

   - **Otimização de uso da E/S de disco**
   - **RAM usada para otimização (400 - 9999 MB)**

5. Configure a programação da tarefa na seção **Agendamento** (é possível configurar uma programação para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).

6. Na janela **<Nome da tarefa>**, clique em **OK**.

Configuração de diagnóstico de travamento no plug-in da Web

Caso ocorra um problema ao operar o Kaspersky Embedded Systems Security for Windows (por exemplo, o aplicativo travar), é possível resolver o problema. Para fazer isso, é possível ativar a criação de arquivos de rastreamento e um arquivo de despejo para o processo do Kaspersky Embedded Systems Security for Windows e enviar esses arquivos para análise ao Suporte Técnico.

O Kaspersky Embedded Systems Security for Windows não envia nenhum arquivo de rastreamento ou de despejo automaticamente. Os dados de diagnóstico só podem ser enviados por um usuário com as permissões necessárias.

O Kaspersky Embedded Systems Security for Windows grava as informações nos arquivos de rastreamento e no arquivo de despejo no formulário 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 for Windows. É possível configurar as permissões de acesso e permitir que apenas os usuários necessários acessem os logs, arquivos de rastreamento e de despejo.

Para definir configurações de diagnóstico de travamento no Kaspersky Security Center:

1. No Console de Administração do Kaspersky Security Center, abra a janela **Configurações do aplicativo**.
2. Abra a seção **Diagnóstico de mau funcionamento**.
3. Para registrar informações de depuração em um arquivo, na seção **Configurações de solução de problemas**, marque a caixa de seleção **Ativar rastreamento**.
4. No campo **Pasta para rastreamento de arquivos**, especifique o caminho absoluto para uma pasta local onde o Kaspersky Embedded Systems Security for Windows salvará os arquivos de rastreamento.

   A pasta deve ser criada com antecedência e deve ter permissão de gravação pela conta SYSTEM. Não é possível especificar uma pasta de rede, uma unidade ou variáveis de ambiente.
5. Configure o nível de detalhe das informações de depuração.
6. Especifique o **Tamanho máximo de arquivos de rastreamento (MB)**.

   Valores disponíveis: de 1 a 4095 MB. Por padrão, o tamanho máximo dos arquivos de rastreamento é definido como 50 MB.
7. Para excluir os arquivos de rastreamento mais antigos quando o número máximo de arquivos for atingido, marque a caixa de seleção **Remover os arquivos de rastreamento mais antigos**.
8. Especifique o **Número máximo de arquivos para um log de rastreamento**.

   Valores disponíveis: de 1 a 999. Por padrão, o número máximo de arquivos é cinco. O campo estará disponível se a caixa de seleção **Remover os arquivos de rastreamento mais antigos** estiver marcada.
9. Se desejar que o aplicativo crie um arquivo de despejo, selecione a caixa **Criar arquivo de despejo**.
10. No campo **Pasta de arquivos de despejo**, especifique o caminho absoluto para uma pasta local onde o Kaspersky Embedded Systems Security for Windows salvará o arquivo de despejo.

    A pasta deve ser criada com antecedência e deve ter permissão de gravação pela conta SYSTEM. Não é possível especificar uma pasta de rede, uma unidade ou variáveis de ambiente.

11. Clique no botão **OK**.

As configurações do aplicativo definidas são aplicadas no dispositivo protegido.

Gerenciando programações de tarefas

Você pode configurar a programação de inicialização para tarefas do Kaspersky Embedded Systems Security for Windows e definir as configurações para executar tarefas com base em uma programação.

Programação de tarefas

É possível programar tarefas locais do sistema e tarefas personalizadas no Console do Aplicativo. Não é possível programar tarefas de grupo no Console do Aplicativo.

Para programar as tarefas de grupo utilizando o plug-in da Web:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Tarefas**.
2. Clique no nome da tarefa na lista de tarefas do Kaspersky Security Center.
   A janela **<Nome da tarefa>** é exibida.
3. Selecione a seção **Configurações do aplicativo**.
4. Na seção **Agendamento**, marque a caixa de seleção **Executar de acordo com o agendamento**.

   Os campos com configurações de programação para as tarefas de Verificação por Demanda e de Atualização estarão indisponíveis caso a programação dessas tarefas seja bloqueada por uma política do Kaspersky Security Center.

5. 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 nos quais a tarefa será iniciada (por padrão, as tarefas são executadas nas segundas-feiras).
   - **Ao iniciar o aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security for Windows.
   - **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 quando a programação inicia.

6. Na seção **Configurações de interrupção de tarefa**:

   a. Marque a caixa de seleção **Duração** e, nos campos à direita, insira o número máximo de horas e minutos da execução da tarefa.

   b. Marque a caixa de seleção **Pausar tarefa** e, nos campos à direita, insira os valores iniciais e finais de um intervalo de tempo menor que 24 horas durante o qual a execução da tarefa será pausada.

7. No bloco **Configurações de agendamento avançadas**:

   a. Marque a caixa de seleção **Cancelar agendamento** 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 **Randomizar o horário de início da tarefa dentro do intervalo** e especifique um valor em minutos.

8. Clique no botão **Salvar** 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 inicialização da tarefa:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Tarefas**.
2. Clique no nome da tarefa na lista de tarefas do Kaspersky Security Center.
   A janela **<Nome da tarefa>** é exibida.
3. Selecione a seção **Configurações do aplicativo**.
4. Selecione a seção **Agendamento**.
5. Execute uma das seguintes ações:

   - Marque a caixa de seleção **Executar de acordo com o agendamento** se desejar ativar a programação de inicialização da tarefa.
   - Desmarque a caixa de seleção **Executar de acordo com o agendamento** se desejar desativar a programação de inicialização da tarefa.

   > As configurações da programação de inicialização da tarefa não são excluídas e serão aplicadas na próxima vez que a inicialização programada de uma tarefa for ativada.

6. Clique no botão **Salvar**.

As definições de programação de inicialização da tarefa configuradas são salvas.

Relatórios no 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 for Windows:

- 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 sobre o status de componentes do Kaspersky Embedded Systems Security for Windows

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: *Em execução*, *Pausado*, *Interrompido*, *Mau funcionamento*, *Não instalado*, *Iniciando*.

O status *Não instalado* refere-se ao componente, não ao próprio aplicativo. Caso o aplicativo não esteja instalado, o Kaspersky Security Center Web Console atribuirá o status N/A (Não disponível).

É possível criar seleções de componentes e usar filtros para exibir dispositivos de rede com um conjunto de componentes especificado e o estado deles.

Consulte a *Ajuda do Kaspersky Security Center* para obter informações detalhadas sobre a criação e o uso das seleções.

Para analisar o status dos componentes nas configurações do aplicativo:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo protegido.
3. Na guia **Geral**, selecione a seção **Componentes**.
4. Revise a tabela de status.

   As informações sobre o status do componente Prevenção de Exploits não estão disponíveis nesta tabela.

Para revisar um relatório padrão do Kaspersky Security Center Web Console:

1. Selecione **Monitoramento e Relatórios → Relatórios**.
2. Selecione o item **Relatório sobre o status dos componentes do aplicativo** da lista e clique no botão **Mostrar relatório**.

   Um relatório é gerado.
3. 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 proibidos nos modos Ativa e de teste

Com base nos resultados da tarefa de Controle de Inicialização de Aplicativos, dois tipos de relatórios podem ser gerados: o relatório de aplicativos proibidos (se a tarefa for iniciada no modo Ativa) e um 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 dispositivos protegidos da rede. Cada relatório é gerado para todos os grupos de administração e acumula dados de todos os aplicativos da Kaspersky instalados nos dispositivos protegidos.

Para revisar um relatório de aplicativos proibidos no modo Somente Estatísticas:

1. Inicie a tarefa de Controle de Inicialização de Aplicativos no modo Somente estatísticas.
2. Selecione **Monitoramento e Relatórios → Relatórios**.
3. Selecione o item **Relatório sobre os aplicativos proibidos no modo de teste** da lista e clique no botão **Mostrar relatório**.

   Um relatório é gerado.
4. Revise os seguintes detalhes do relatório:

   - Um diagrama gráfico que exibe os 10 aplicativos com o maior número de inicializações bloqueadas.
   - Uma tabela de resumo de bloqueios de aplicativos 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 Ativa:

1. Inicie a tarefa de Controle de Inicialização de Aplicativos no modo Ativa.
2. Selecione **Monitoramento e Relatórios → Relatórios**.
3. Selecione o item **Relatório sobre os aplicativos proibidos no modo de teste** da lista e clique no botão **Mostrar relatório**.

   Um relatório é gerado.

Este relatório contém os mesmos dados sobre blocos que o relatório de aplicativos proibidos no modo de teste.

Interface de diagnóstico compacta

Esta seção descreve como usar a Interface de diagnóstico compacta para revisar o status do dispositivo protegido ou a atividade atual, e como configurar a escrita de arquivos de despejo e rastreamento.

Sobre a interface de diagnóstico compacta

O componente Interface de diagnóstico compacta (também referido como "CDI") é instalado e desinstalado junto com o componente Ícone da bandeja do sistema, independentemente do Console do Aplicativo, e pode ser usado quando o Console do Aplicativo não estiver instalado no dispositivo protegido. A Interface de Diagnóstico Compacta é iniciada a partir do Ícone da Bandeja do Sistema ou pela execução do arquivo kavfsmui.exe na pasta do aplicativo no dispositivo protegido.

Na Interface de Diagnóstico Compacta é possível fazer o seguinte:

- Analisar informações sobre o status geral do aplicativo.
- Revisar incidentes de segurança que ocorreram.
- Analisar a atividade atual no dispositivo protegido.
- Iniciar ou interromper a escrita de arquivos de despejo e de rastreamento.
- Abrir o Console do Aplicativo.
- Abra a janela **Sobre o aplicativo** com a lista de atualizações instaladas e patches disponíveis.

A Interface de Diagnóstico Compacta está disponível mesmo se o acesso às funções do Kaspersky Embedded Systems Security for Windows for protegido por senha. Nenhuma senha é necessária.

O componente Interface de Diagnóstico Compacta não pode ser configurado pelo Kaspersky Security Center.

Revisão do status do Kaspersky Embedded Systems Security for Windows por meio da Interface de diagnóstico compacta

Para abrir a janela da Interface de Diagnóstico Compacta, execute as seguintes ações:

1. Clique com o botão direito do mouse no ícone da bandeja do sistema do Kaspersky Embedded Systems Security for Windows na área de notificação de barra de ferramentas.
2. Selecione a opção **Abrir Interface de diagnóstico compacta**.

   A **Interface de diagnóstico compacta** é exibida.

Revise o status atual da chave, as tarefas de Proteção do Computador em Tempo Real e as tarefas de Atualização na guia **Status de proteção**. As cores diferentes são usadas para notificar o usuário sobre o status de proteção (ver a tabela abaixo).

Status de proteção na Interface de Diagnóstico Compacta

Seção	Status

Status de proteção em tempo real	O painel fica *verde* para qualquer um dos seguintes cenários (se qualquer uma das condições for atendida):
	• Configuração recomendada:
	  • A tarefa de Proteção de Arquivos em Tempo Real é iniciada com as configurações padrão.
	  • A tarefa de Controle de Inicialização de Aplicativos é iniciada no modo **Ativa** com as configurações padrão.
	• Configuração aceitável:
	  • A tarefa de Proteção de Arquivos em Tempo Real é configurada pelo usuário.
	  • As configurações da tarefa de Controle de Inicialização de Aplicativos são modificadas.

	O painel fica *amarelo* se uma ou mais das seguintes condições forem atendidas: • A tarefa de Proteção de Arquivos em Tempo Real é pausada (pelo usuário ou programação). • A tarefa de Controle de Inicialização de Aplicativos é iniciada no modo **Somente estatísticas**. • A Prevenção de Exploits e o Controle de Inicialização de Aplicativos são iniciados no modo **Somente estatísticas**.
	O painel fica *vermelho* se as seguintes condições forem atendidas: • O componente de Proteção de Arquivos em Tempo Real não está instalado ou a tarefa é interrompida ou pausada. • O componente Controle de Inicialização de Aplicativos não está instalado ou a tarefa é iniciada no modo **Somente estatísticas**.
Licenciamento	O painel fica *verde* se a licença atual for válida.
	Um painel *amarelo* significa que um dos seguintes eventos ocorreu: • *Verificação do status da licença.* • *A licença expirará em 14 dias e nenhuma chave adicional ou código de ativação foi adicionado.* • *A chave adicionada foi colocada na lista de bloqueio e está prestes a ser bloqueada.*
	Um painel *vermelho* significa que um dos seguintes eventos ocorreu: • *Aplicativo não ativado* • *A licença expirou* • *O Contrato de licença do usuário final foi violado*

	• *A chave está na lista de bloqueio*
Atualização	O painel fica *verde* quando os bancos de dados do aplicativo estão atualizados.
	O painel fica *amarelo* quando os bancos de dados do aplicativo estão desatualizados.
	O painel fica *vermelho* quando os bancos de dados do aplicativo estão muito desatualizados.

Revisando estatística de evento de segurança

A guia **Estatísticas** exibe todos os eventos de segurança. Cada estatística de tarefa de proteção é exibida em um bloco separado que especifica o número de incidentes, a data e a hora quando o último incidente ocorreu. Quando um incidente é registrado em log, a cor do bloco se altera para vermelho.

Para revisar as estatísticas:

1. Clique com o botão direito do mouse no ícone da bandeja do sistema do Kaspersky Embedded Systems Security for Windows na área de notificação de barra de ferramentas.
2. Selecione a opção **Abrir Interface de diagnóstico compacta**.

   A **Interface de diagnóstico compacta** é exibida.
3. Abra a guia **Estatísticas**.
4. Revise os incidentes de segurança para as tarefas de proteção.

Revisando a atividade atual do aplicativo

Nesta guia, é possível revisar o status das tarefas atuais e os processos do aplicativo, e receber notificações prontamente sobre eventos críticos que venham a ocorrer.

As cores diferentes são usadas para indicar o status de atividade do aplicativo:

- Na seção **Tarefas**:
  - *Verde*. Nenhuma condição requer amarelo ou vermelho.
  - *Amarelo*. As áreas críticas não são verificadas há muito tempo.
  - *Vermelho*. Pelo menos uma das seguintes condições é verdadeira:
    - Nenhuma tarefa foi iniciada e uma programação de início não foi configurada para nenhuma tarefa.
    - Os erros de inicialização de aplicativos são registrados como eventos críticos.
- Na seção **Kaspersky Security Network**:
  - *Verde*. A tarefa de Uso da KSN é iniciada.

- *Amarelo*. A Declaração da KSN é aceita, mas a tarefa não é iniciada.

Para revisar a atividade atual do aplicativo no dispositivo protegido:

1. Clique com o botão direito do mouse no ícone da bandeja do sistema do Kaspersky Embedded Systems Security for Windows na área de notificação de barra de ferramentas.
2. Selecione a opção **Abrir Interface de diagnóstico compacta**.

   A **Interface de diagnóstico compacta** é exibida.
3. Abrir a guia **Atividade do aplicativo atual**.
4. Revise as seguintes informações na seção **Tarefas**:
   - **Áreas críticas não verificados há muito tempo**.

     Este campo é exibido apenas se o aplicativo retornar um aviso correspondente sobre a verificações de áreas críticas.
   - **Funcionando agora**
   - **Execução falhou**
   - **Próximo início definido por um agendamento**
5. Revise as seguintes informações na seção **Kaspersky Security Network**:
   - **KSN está ligado. Serviços de reputação de arquivo estão ativados** ou a **Proteção está desligada**.
   - **KSN está ligado. Serviços de reputação de arquivo estão ativados**, **estatísticas do aplicativo está sendo enviado para KSN**.

     O aplicativo envia informações sobre malwares, inclusive softwares fraudulentos, detectadas durante a execução das tarefas de Proteção de arquivos em tempo real e Verificação por demanda, assim como as informações de depuração sobre erros durante a verificação.

     O campo é exibido se a caixa de seleção **Enviar as estatísticas da Kaspersky Security Network** for marcada nas configurações da tarefa de Uso da KSN.
6. Revise as seguintes informações na seção **Integração com o Kaspersky Security Center**:
   - **Gerenciamento local é permitido**.
   - **Política está aplicada: <Nome do Servidor de Administração>**.

Configuração da escrita de arquivos de despejo e de rastreamento

É possível configurar a gravação de arquivos de despejo e de rastreamento na Interface de Diagnóstico Compacta.

Você também pode configurar o diagnóstico de mau funcionamento por meio do Console do Aplicativo.

Para iniciar a escrita em arquivos de despejo e de rastreamento, execute as seguintes ações:

1. Clique com o botão direito do mouse no ícone da bandeja do sistema do Kaspersky Embedded Systems Security for Windows na área de notificação de barra de ferramentas.
2. Selecione a opção **Abrir Interface de diagnóstico compacta**.

   A **Interface de diagnóstico compacta** é exibida.
3. Abra a guia **Solução de problemas**.
4. Altere as seguintes configurações de rastreamento, conforme necessário:

   a. Marque a caixa de seleção **Gravar as informações de depuração no arquivo de rastreamento**.

   b. Clique no botão **Procurar** para especificar a pasta na qual o Kaspersky Embedded Systems Security for Windows salvará os arquivos de rastreamento.

   O rastreamento será ativado para todos os componentes com as configurações padrão usando o nível de detalhe *Depuração* e o tamanho de log com o padrão máximo de 50 MB.
5. Altere as seguintes configurações do arquivo de despejo, conforme necessário:

   a. Selecione a caixa **Criar arquivo de despejo sobre mau funcionamento nesta pasta**.

   b. Clique no botão **Procurar** para especificar a pasta na qual o Kaspersky Embedded Systems Security for Windows salvará o arquivo de despejo.
6. Clique no botão **Aplicar**.

   A nova configuração será aplicada.

Atualização do banco de dados e dos módulos de software do Kaspersky Embedded Systems Security for Windows

Essa seção fornece informações sobre as tarefas de atualização dos bancos de dados e dos módulos de software do Kaspersky Embedded Systems Security for Windows, a cópia de atualizações e a reversão de atualização do banco de dados do Kaspersky Embedded Systems Security for Windows, bem como instruções sobre como configurar as tarefas de atualização do banco de dados e dos módulos de software.

Sobre as tarefas de atualização

O Kaspersky Embedded Systems Security for Windows fornece quatro tarefas de atualização do sistema: Atualização do Banco de Dados, Atualização dos Módulos de Software, Copiar atualizações e Reversão da atualização do banco de dados.

Por padrão, o Kaspersky Embedded Systems Security for Windows conecta-se à fonte de atualização (um dos servidores de atualização da Kaspersky) a cada hora. Você pode configurar todas as tarefas de Atualização, exceto a tarefa de Reversão da Atualização do Banco de Dados. Quando as configurações da tarefa forem modificadas, o Kaspersky Embedded Systems Security for Windows aplicará os novos valores na próxima execução da tarefa.

Não é permitido fazer uma pausa e reiniciar as tarefas de atualização.

Atualização do Banco de Dados

O Kaspersky Embedded Systems Security for Windows copia bancos de dados a partir da fonte de atualização para o dispositivo e começa a usá-los imediatamente na tarefa de Proteção do Computador em Tempo Real em execução. As tarefas de Verificação por Demanda começam a usar o banco de dados atualizado na próxima execução.

Por padrão, o Kaspersky Embedded Systems Security for Windows executa a tarefa de Atualização do banco de dados de hora em hora.

Atualização dos Módulos de Software

Por padrão, o Kaspersky Embedded Systems Security for Windows verifica a disponibilidade de atualizações dos módulos de software na fonte de atualização. Para começar a usar os módulos de software instalados, é necessário reiniciar o dispositivo protegido e/ou o Kaspersky Embedded Systems Security for Windows.

Por padrão, o Kaspersky Embedded Systems Security for Windows executa a tarefa de Atualização dos módulos de software semanalmente às sextas-feiras às 16h00 (de acordo com as configurações de hora regionais do dispositivo protegido). Durante a execução da tarefa, o aplicativo verifica a disponibilidade de atualizações importantes e programas de módulos do Kaspersky Embedded Systems Security for Windows sem distribuí-las.

Copiar atualizações

Por padrão, durante a execução da tarefa, o Kaspersky Embedded Systems Security for Windows faz o download dos arquivos da Atualização do banco de dados e os salva na rede especificada ou pasta local sem aplicá-los.

A tarefa Copiar atualizações está desativada por padrão.

Reversão da Atualização do Banco de Dados

Durante a execução da tarefa, o Kaspersky Embedded Systems Security for Windows volta a utilizar os bancos de dados de atualizações instaladas previamente.

A tarefa de Reversão da atualização do banco de dados está desativada por padrão.

Sobre a Atualização dos Módulos de Software

A Kaspersky pode publicar pacotes de atualização para módulos do Kaspersky Embedded Systems Security for Windows. Os pacotes de atualização podem ser *urgentes* (ou *críticos*) ou planejados. Os pacotes de atualização críticos corrigem vulnerabilidades e erros; os pacotes planejados adicionam novos recursos ou aprimoram recursos existentes.

Os pacotes de atualização urgentes (críticos) são carregados nos servidores de atualização da Kaspersky. A sua instalação automática pode ser configurada usando a tarefa de Atualização dos módulos de software. Por padrão, o Kaspersky Embedded Systems Security for Windows executa a tarefa de Atualização dos módulos de software semanalmente às sextas-feiras às 16h00 (de acordo com as configurações de hora regionais do dispositivo protegido).

A Kaspersky não publica pacotes de atualizações planejados nos servidores de atualização para atualização automática; eles podem ser baixados no site da Kaspersky. A tarefa de Atualização dos módulos de software pode ser usada para receber informações sobre a versão de atualizações programadas do Kaspersky Embedded Systems Security for Windows.

É possível baixar atualizações críticas da Internet para cada dispositivo protegido ou é possível usar um único dispositivo protegido como intermediário copiando todas as atualizações para ele e depois distribuindo-as entre os dispositivos protegidos na rede. Para copiar e salvar atualizações sem instalá-las, use a tarefa Copiar atualizações.

Antes da instalação das atualizações dos módulos, o Kaspersky Embedded Systems Security for Windows cria cópias de backup dos módulos instalados anteriormente. Se o processo de atualização dos módulos de software for interrompido ou resultar em erro, o Kaspersky Embedded Systems Security for Windows retornará automaticamente ao uso dos módulos de software instalados anteriormente. Os módulos do software podem ser revertidos manualmente para as atualizações instaladas anteriormente.

Durante a instalação das atualizações baixadas, o Kaspersky Security Service é interrompido e reiniciado automaticamente.

Sobre a atualização do banco de dados

Os bancos de dados do Kaspersky Embedded Systems Security for Windows armazenados no dispositivo protegido ficam desatualizados rapidamente. Os analistas de vírus da Kaspersky detectam novas ameaças diariamente, criam registros para identificá-las e trabalham para incluí-las nas atualizações do banco de dados do aplicativo. As atualizações do banco de dados são um arquivo ou um conjunto de arquivos contendo registros que identificam as ameaças descobertas no período desde a criação da última atualização. Para manter o nível necessário de proteção do dispositivo, é recomendado que atualizações do banco de dados sejam recebidas periodicamente.

Por padrão, se os bancos de dados do Kaspersky Embedded Systems Security for Windows não forem atualizados até uma semana depois que as atualizações do banco de dados instaladas foram criadas, ocorrerá o evento *O banco de dados do aplicativo está desatualizado*. Se os bancos de dados não forem atualizados durante um período de duas semanas, ocorrerá o evento *O banco de dados do aplicativo está muito desatualizado*. As informações sobre o status de atualização dos bancos de dados são exibidas no painel de resultados do node do **Kaspersky Embedded Systems Security for Windows** na árvore do Console do Aplicativo. Você pode usar as configurações gerais do Kaspersky Embedded Systems Security for Windows para indicar um número diferente de dias antes que estes eventos ocorram. Você também pode configurar notificações de administrador sobre estes eventos.

O Kaspersky Embedded Systems Security for Windows baixa atualizações de bancos de dados e módulos do aplicativo a partir dos servidores de atualização FTP ou HTTP da Kaspersky, do Servidor de Administração do Kaspersky Security Center ou de outras fontes de atualização.

É possível baixar as atualizações para cada dispositivo protegido ou usar um dispositivo protegido como intermediário. As atualizações serão copiadas para ele e, em seguida, distribuídas para os dispositivos protegidos. Se você usar o Kaspersky Security Center para administração centralizada da proteção de dispositivos em uma organização, poderá usar o Servidor de Administração do Kaspersky Security Center como intermediário para baixar atualizações.

As tarefas de Atualização do banco de dados podem ser iniciadas manualmente ou com base em uma programação. Por padrão, o Kaspersky Embedded Systems Security for Windows executa a tarefa de Atualização do banco de dados de hora em hora.

Se o processo de download da atualização for interrompido ou resultar em erro, o Kaspersky Embedded Systems Security for Windows retornará automaticamente ao uso dos bancos de dados de atualizações instaladas anteriormente. Se os bancos de dados do Kaspersky Embedded Systems Security for Windows forem corrompidos, eles podem ser revertidos manualmente para as atualizações instaladas anteriormente.

Esquemas para atualizar bancos de dados e módulos de aplicativos antivírus usados em uma organização

A seleção de uma fonte de atualização nas tarefas de atualização depende do esquema usado para atualizar bancos de dados e módulos do programa na organização.

Os bancos de dados e módulos do Kaspersky Embedded Systems Security for Windows podem ser atualizados nos dispositivos protegidos usando os seguintes esquemas:

- Baixar as atualizações diretamente da Internet para cada dispositivo protegido (Esquema 1).
- Baixar as atualizações da Internet para um dispositivo intermediário e distribuí-las para dispositivos protegidos a partir do dispositivo.

  Qualquer dispositivo com os softwares listados abaixo instalados pode ser usado como um dispositivo intermediário:

  - Kaspersky Embedded Systems Security for Windows (Esquema 2).
  - Servidor de Administração do Kaspersky Security Center (Esquema 3).

Atualizar usando um dispositivo intermediário não só diminui o tráfego da Internet, mas também fornece segurança adicional ao dispositivo protegido da rede.

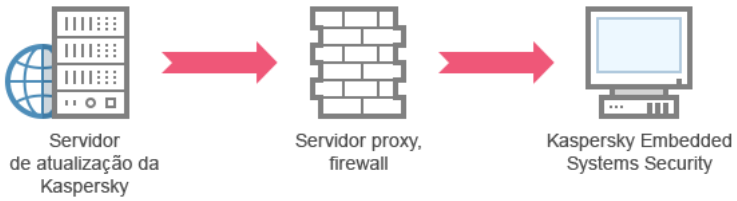
Os esquemas de atualização listados estão descritos abaixo.

Esquema 1. Atualização dos bancos de dados e módulos diretamente da Internet

Para configurar atualizações do Kaspersky Embedded Systems Security for Windows diretamente da Internet:

em cada dispositivo protegido nas configurações da tarefa de Atualização do banco de dados e na tarefa de Atualização dos módulos de software, especifique os servidores de atualização da Kaspersky como a fonte de atualização.

Outros servidores HTTP ou FTP que têm uma pasta de atualização podem ser configurados como fonte de atualização.



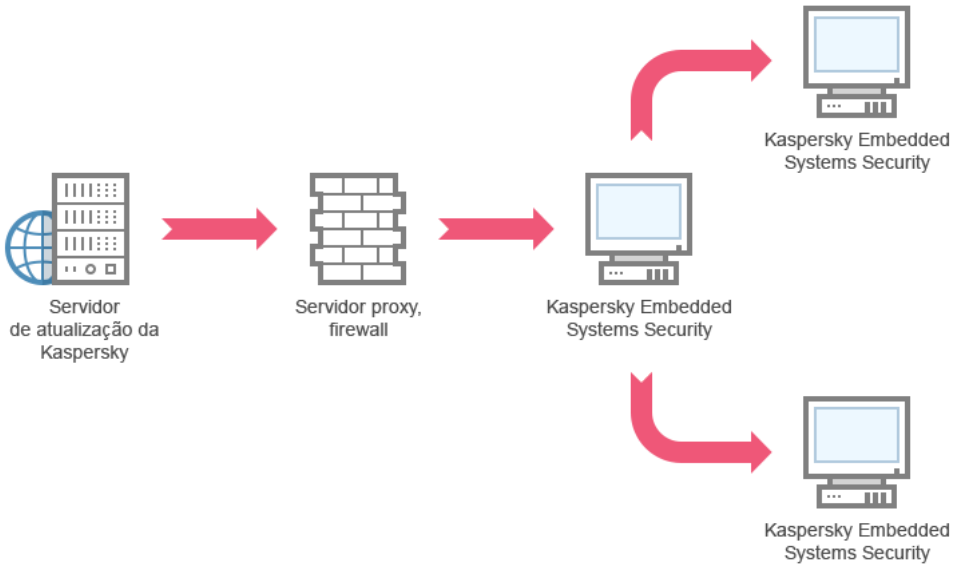
Esquema 1: atualização dos bancos de dados e módulos diretamente da Internet

Esquema 2. Atualização dos bancos de dados e módulos através de um dos dispositivos protegidos

Para configurar atualizações do Kaspersky Embedded Systems Security for Windows através de um dos dispositivos protegidos:

1. Copie as atualizações para o dispositivo protegido selecionado. Para isso, execute as seguintes ações:
   - Configure a tarefa Copiar atualizações no dispositivo protegido selecionado:
     a. Especifique o servidor de atualização da Kaspersky como fonte de atualizações.
     b. Especifique uma pasta compartilhada a ser usada como a pasta onde as atualizações são salvas.
2. Distribua as atualizações para outros dispositivos protegidos. Para isso, execute as seguintes ações:
   - Em cada dispositivo protegido, defina as configurações para a tarefa de Atualização do Banco de Dados e para a tarefa de Atualização dos Módulos de Software (consulte a figura abaixo).
     a. Para a fonte de atualização, especifique uma pasta na unidade do dispositivo intermediário na qual as atualizações serão baixadas.

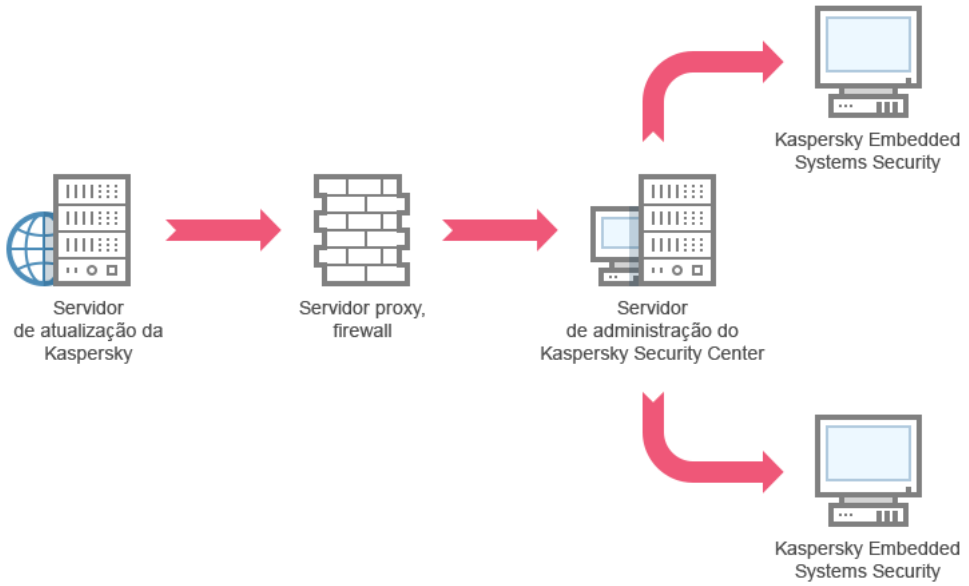
O Kaspersky Embedded Systems Security for Windows obterá atualizações através de um dos dispositivos protegidos.



Esquema 2: atualização dos bancos de dados e módulos por um dos dispositivos protegidos

Esquema 3. Atualização dos bancos de dados e módulos através do Servidor de Administração do Kaspersky Security Center

Se o Kaspersky Security Center for usado para a administração centralizada da proteção antivírus do dispositivo, as atualizações poderão ser baixadas através do Servidor de Administração do Kaspersky Security Center instalado na rede de área local (consulte a figura abaixo).



Esquema 3: atualização dos bancos de dados e módulos pelo Servidor de Administração do Kaspersky Security Center

Para configurar atualizações do Kaspersky Embedded Systems Security for Windows através do Servidor de Administração do Kaspersky Security Center:

1. Baixe atualizações dos servidores de atualização da Kaspersky para o Servidor de Administração do Kaspersky Security Center. Para isso, execute as seguintes ações:

   - Configure a tarefa Recuperar atualizações pelo Servidor de administração para o conjunto de dispositivos protegidos especificado:

     a. Especifique o servidor de atualização da Kaspersky como fonte de atualizações.

2. Distribua atualizações para os dispositivos protegidos. Para fazer isso, execute uma das seguintes ações:

- No Kaspersky Security Center, configure uma tarefa de grupo de atualização (módulo do aplicativo) do banco de dados de antivírus para distribuir atualizações para os dispositivos protegidos:

  a. Na programação da tarefa, especifique **Após o Servidor de Administração ter recuperado as atualizações** como frequência de início.

  O Servidor de Administração executará a tarefa sempre que receber atualizações (método recomendado).

  A frequência de início **Após o Servidor de Administração ter recuperado as atualizações** não pode ser especificada no Console do Aplicativo.

- Em cada dispositivo protegido, configure a tarefa de Atualização do banco de dados e a tarefa de Atualização dos módulos de software:

  a. Especifique o Servidor de Administração do Kaspersky Security Center como a fonte de atualização.

  b. Configure a programação da tarefa se necessário.

  Se os bancos de dados de antivírus do Kaspersky Embedded Systems Security for Windows forem raramente atualizados (de uma vez por mês a uma vez por ano), a probabilidade da detecção de ameaças cai e a frequência de falsos positivos é elevada pelos aumentos dos componentes do aplicativo.

O Kaspersky Embedded Systems Security for Windows obterá atualizações através do Servidor de Administração do Kaspersky Security Center.

Caso pretenda usar o Servidor de Administração do Kaspersky Security Center para distribuir atualizações, instale o Agente de rede (um componente do aplicativo incluído no kit de distribuição do Kaspersky Security Center) em cada um dos dispositivos protegidos. Isso garante a interação entre o Servidor de Administração e o Kaspersky Embedded Systems Security for Windows no dispositivo protegido. Informações detalhadas sobre o Agente de rede e sua configuração usando o Kaspersky Security Center são fornecidas na *Ajuda do Kaspersky Security Center*.

Configurando tarefas de atualização

Esta seção fornece instruções sobre como configurar tarefas de atualização do Kaspersky Embedded Systems Security for Windows.

Definindo as configurações para trabalhar com fontes de atualização do Kaspersky Embedded Systems Security for Windows

Para cada tarefa de atualização, exceto a tarefa de Reversão da atualização do banco de dados, é possível especificar uma ou mais fontes de atualização, adicionar fontes de atualização definidas pelo usuário e definir as configurações para a conexão com as fontes especificadas.

Depois que as configurações da tarefa de atualização forem modificadas, as novas configurações não serão imediatamente aplicadas nas tarefas de atualização em execução. As configurações definidas serão aplicadas somente quando a tarefa for reiniciada.

Para especificar o tipo de fonte de atualização:

1. Na árvore do Console do Aplicativo, expanda o node **Atualização**.
2. Selecione o node secundário que corresponde à tarefa de atualização que deseja configurar.
3. Clique no link **Propriedades** no painel de resultados do node selecionado.

   A janela **Configurações de tarefa** é exibida na guia **Geral**.
4. Na seção **Fonte de atualização**, selecione o tipo de fonte de atualização do Kaspersky Embedded Systems Security for Windows:
   - **Servidor de Administração do Kaspersky Security Center**
   - **Servidores de atualização da Kaspersky**
   - **Servidores HTTP ou FTP ou pastas de rede personalizados**
5. Se necessário, defina as configurações avançadas para as fontes de atualização definidas pelo usuário:
   a. Clique no link **Servidores HTTP ou FTP ou pastas de rede personalizados**.
      1. Na janela **Servidores de atualização** exibida, selecione ou desmarque as caixas ao lado das fontes de atualização definidas pelo usuário para começar ou interromper seu uso.
      2. Clique no botão **OK**.
   b. Na seção **Fonte de atualização** na guia **Geral**, selecione ou desmarque a caixa de seleção **Usar servidores de atualização da Kaspersky se os servidores especificados não estiverem disponíveis**.
6. Na janela **Configurações de tarefa**, selecione a guia **Configurações de conexão** para definir as configurações para se conectar a fontes de atualização:
   - Desmarque ou marque a caixa de seleção **Usar configurações do servidor proxy para conectar aos servidores de atualização da Kaspersky**.
   - Desmarque ou marque a caixa de seleção **Usar configurações de servidor proxy para conectar a outros servidores**.

   Para obter informações sobre a definição de configurações opcionais do servidor proxy e autenticação para acesso ao servidor proxy, consulte a seção Inicialização e configuração da tarefa de Atualização do Banco de Dados do Kaspersky Embedded Systems Security for Windows.
7. Clique no botão **OK**.

As configurações definidas para a fonte de atualização do Kaspersky Embedded Systems Security for Windows serão salvas e aplicadas no momento da próxima inicialização da tarefa.

Você pode gerenciar a lista de fontes de atualização do Kaspersky Embedded Systems Security for Windows definida pelo usuário.

Para editar a lista de fontes de atualização de aplicativo definida pelo usuário:

1. Na árvore do Console do Aplicativo, expanda o node **Atualização**.
2. Selecione o node secundário que corresponde à tarefa de atualização que deseja configurar.
3. Clique no link **Propriedades** no painel de resultados do node selecionado.

   A janela **Configurações de tarefa** é exibida na guia **Geral**.
4. Clique no link **Servidores HTTP ou FTP ou pastas de rede personalizados**.

   A janela **Servidores de atualização** é exibida.
5. Faça o seguinte:

   - Para adicionar uma nova fonte de atualização definida pelo usuário, clique em **Adicionar** e, no campo de entrada, especifique o endereço da pasta que contém os arquivos de atualização no servidor FTP ou HTTP. Especifique uma pasta local ou de rede no formato UNC (Universal Naming Convention). Pressione a tecla **ENTER**.

     Por padrão, a pasta adicionada é usada como a fonte de atualização.
   - Para desativar o uso de uma fonte definida pelo usuário, desmarque a caixa ao lado da fonte na lista.
   - Para ativar o uso de uma fonte definida pelo usuário, selecione a caixa ao lado da fonte na lista.
   - Para alterar a ordem na qual o Kaspersky Embedded Systems Security for Windows acessa fontes de atualização definidas pelo usuário, use os botões **Mover para cima** e **Mover para baixo** para mover a fonte selecionada em direção ao início ou final da lista, para que ela seja usada antes ou depois de outras fontes.
   - Para alterar o caminho para uma fonte definida pelo usuário, selecione a fonte na lista e clique no botão **Editar**, efetue as alterações necessárias no campo de entrada e pressione a tecla **ENTER**.
   - Para remover uma fonte definida pelo usuário, selecione-a na lista e clique no botão **Remover**.

     Não é possível excluir a única fonte definida pelo usuário da lista.
6. Clique no botão **OK**.

As modificações na lista de fontes de atualização de aplicativo definidas pelo usuário serão salvas.

Otimização da E/S de disco ao executar a tarefa de Atualização do banco de dados

Ao executar a tarefa de Atualização do banco de dados, o Kaspersky Embedded Systems Security for Windows armazena arquivos de atualização na unidade local do dispositivo protegido. É possível diminuir a carga de trabalho no subsistema de E/S de disco do dispositivo protegido por meio do armazenamento de arquivos de atualização em uma unidade virtual na RAM ao executar a tarefa de atualização.

Este recurso está disponível para os sistemas operacionais Microsoft Windows 7 e posteriores.

Ao usar este recurso executando a tarefa de Atualização do banco de dados, uma unidade lógica extra pode aparecer no sistema operacional. Esta unidade lógica será removida do sistema operacional após a tarefa ser concluída.

Para diminuir a carga de trabalho no subsistema de E/S de disco dos dispositivos protegidos durante a tarefa de Atualização do Banco de Dados:

1. Na árvore do Console do Aplicativo, expanda o node **Atualização**.
2. Selecionar o node secundário **Atualização do Banco de Dados**.
3. Clique no link **Atualização do Banco de Dados** no painel de resultados do node **Propriedades**.

   A janela **Configurações de tarefa** é exibida na guia **Geral**.
4. Na seção **Otimização de uso da E/S de disco**, defina as seguintes configurações:
   - Desmarque ou marque a caixa de seleção **Diminuir a carga na E/S de disco**.
   - No campo **RAM usada para otimização, MB**, especifique o volume de RAM (em MB). O sistema operacional aloca temporariamente o volume de RAM especificado para armazenar arquivos de atualização ao executar a tarefa. O tamanho de RAM padrão é 512 MB. O tamanho de RAM padrão é 400 MB.

     Ao executar a tarefa de Atualização do Banco de Dados com o recurso de otimização do subsistema de disco ativado, pode ocorrer um dos seguintes casos, dependendo da quantidade de RAM alocada para o recurso:

     - Se o valor for muito pequeno, a quantidade de RAM alocada poderá ser insuficiente para concluir a tarefa de atualização do banco de dados (por exemplo, durante a primeira atualização), o que levará à conclusão da tarefa com um erro.

       Nesse caso, é recomendado alocar mais RAM para o recurso de otimização do subsistema de disco.
     - Caso o valor seja muito grande, no início da tarefa de atualização do banco de dados, talvez seja impossível criar uma unidade virtual com um tamanho selecionado na RAM. Consequentemente, o recurso de otimização do subsistema de disco é desativado automaticamente, e a tarefa de atualização do banco de dados é executada sem o recurso de otimização.

       Nesse caso, é recomendado alocar menos RAM para o recurso de otimização do subsistema de disco.
5. Clique no botão **OK**.

As configurações definidas serão salvas e aplicadas na próxima inicialização da tarefa.

Configuração da tarefa Copiar atualizações

Para configurar a tarefa Copiar atualizações:

1. Na árvore do Console do Aplicativo, expanda o node **Atualização**.
2. Selecione o node secundário **Copiar atualizações**.
3. Clique no link **Copiar atualizações** no painel de resultados do node **Propriedades**.

A janela **Configurações de tarefa** é aberta.

4. Nas guias **Geral** e **Configurações de conexão**, defina as configurações para trabalhar com fontes de atualização.

5. Na guia **Geral** na seção **Configurações da cópia de atualizações**:

   - Especifique as condições para copiar atualizações:
     - **Copiar atualizações do banco de dados**.
     - **Copiar atualizações críticas dos módulos de software**.
     - **Copiar atualizações do banco de dados e atualizações críticas dos módulos de software**.
   - Especifique a pasta local ou pasta de rede para a qual o Kaspersky Embedded Systems Security for Windows distribuirá as atualizações baixadas.

6. Nas guias **Agendamento** e **Avançado**, configure a programação de inicialização da tarefa.

7. Na guia **Executar como**, configure a tarefa a ser iniciada usando uma conta de usuário específica.

8. Clique no botão **OK**.

As configurações definidas serão salvas e aplicadas na próxima inicialização da tarefa.

Definindo as Configurações da tarefa de Atualização dos Módulos de Software

Para configurar a tarefa de Atualização dos módulos de software:

1. Na árvore do Console do Aplicativo, expanda o node **Atualização**.

2. Selecione o node secundário **Atualização dos Módulos de Software**.

3. Clique no link **Atualização dos Módulos de Software** no painel de resultados do node **Propriedades**.

   A janela **Configurações de tarefa** é aberta.

4. Nas guias **Geral** e **Configurações de conexão**, defina as configurações para trabalhar com fontes de atualização.

5. Na guia **Geral**, na seção **Configurações de atualização**, defina as configurações para atualizar módulos de aplicativo:

   - **Verificar apenas as atualizações críticas disponíveis dos módulos de software**
   - **Copiar e instalar atualizações críticas dos módulos de software**
   - **Permitir reinício do sistema operacional**
   - **Receber informações sobre as atualizações disponíveis programadas dos módulos de software**

6. Nas guias **Agendamento** e **Avançado**, configure a programação de inicialização da tarefa. Por padrão, o Kaspersky Embedded Systems Security for Windows executa a tarefa de Atualização dos módulos de software

semanalmente às sextas-feiras às 16h00 (de acordo com as configurações de hora regionais do dispositivo protegido).

7. Na guia **Executar como**, configure a tarefa a ser iniciada com o uso de uma conta de usuário específica.

8. Clique no botão **OK**.

As configurações definidas serão salvas e aplicadas na próxima inicialização da tarefa.

A Kaspersky não publica pacotes de atualizações planejados nos servidores de atualização para instalação automática; eles podem ser baixados manualmente no site da Kaspersky. É possível configurar notificações de administrador sobre o evento *Há atualizações críticas e programadas disponíveis*. A notificação conterá o URL da página da Web no qual é possível baixar as atualizações programadas.

Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security for Windows

Antes que as atualizações do banco de dados sejam executadas, o Kaspersky Embedded Systems Security for Windows cria cópias de backup dos bancos de dados usados anteriormente. Se uma atualização for interrompida ou resultar em erro, o Kaspersky Embedded Systems Security for Windows retornará automaticamente ao uso dos bancos de dados instalados anteriormente.

Se algum problema surgir após a atualização dos bancos de dados, será possível reverter às atualizações instaladas anteriormente por meio da tarefa reversão da atualização do banco de dados.

Para iniciar a tarefa Reversão da atualização do banco de dados:

No painel de resultados do node **Reversão da atualização do banco de dados do aplicativo**, clique no link **Iniciar**.

Revertendo atualizações dos módulos do aplicativo

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

Antes de aplicar as atualizações dos módulos de software, o Kaspersky Embedded Systems Security for Windows cria cópias de backup dos módulos atualmente em uso. Se o processo de atualização dos módulos for interrompido ou resultar em erro, o Kaspersky Embedded Systems Security for Windows retornará automaticamente ao uso dos módulos das últimas atualizações instaladas.

Para reverter os módulos de software, use o recurso **Instalar e excluir aplicativos** do Microsoft Windows.

Estatísticas da tarefa de atualização

Enquanto a tarefa de atualização está sendo executada, as informações em tempo real sobre a quantidade de dados baixados desde o início da tarefa são exibidas, além de outras estatísticas de execução da tarefa.

Quando a tarefa for concluída ou interrompida, a informação estará disponível no log de tarefas.

Para exibir as estatísticas da tarefa de atualização:

1. Na árvore do Console do Aplicativo, expanda o node **Atualização**.
2. Selecione o node secundário que corresponde à tarefa cuja estatística deseja visualizar.

As estatísticas de tarefas são exibidas na seção **Estatísticas** do painel de resultados do node selecionado.

Caso esteja visualizando a tarefa de Atualização do banco de dados ou a tarefa Copiar atualizações, a seção **Estatísticas** exibirá o volume de dados baixados pelo Kaspersky Embedded Systems Security for Windows a partir do momento presente (**Dados recebidos**).

A tabela a seguir contém os detalhes da tarefa de atualização dos módulos de software.

Informações sobre a tarefa de Atualização dos Módulos de Software

Campo	Descrição
Dados recebidos	Quantidade total de dados baixados.
Atualizações críticas disponíveis	Número de atualizações críticas disponíveis para instalação.
Atualizações programadas disponíveis	Número de atualizações planejadas disponíveis para instalação.
Erros ao aplicar atualizações	Se o valor deste campo for diferente de zero, a atualização não foi aplicada. O nome da atualização que causou um erro pode ser exibido no log de tarefas.

Isolamento de objetos e cópia de backups

Esta seção fornece informações sobre o backup de objetos maliciosos detectados antes que sejam desinfectados ou removidos, bem como informações sobre a quarentena de objetos possivelmente infectados.

Isolando objetos possivelmente infectados. Quarentena

Essa seção descreve como isolar objetos possivelmente infectados colocando-os na Quarentena e como especificar as configurações da Quarentena.

Sobre colocar em Quarentena objetos possivelmente infectados

O Kaspersky Embedded Systems Security for Windows coloca em Quarentena objetos possivelmente infectados, movendo-os da sua localização original para a pasta de *Quarentena*. Por motivos de segurança, os objetos na pasta Quarentena são armazenados em formato criptografado.

Exibição de objetos em Quarentena

Os objetos da Quarentena podem ser exibidos no node **Quarentena** do Console do Aplicativo.

Para exibir os objetos em Quarentena:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Selecione o node secundário **Quarentena**.

   As informações sobre objetos em quarentena são exibidas no painel de resultados do node selecionado.

Para encontrar o objeto requerido na lista de objetos colocados na quarentena,

classifique os objetos ou filtre os objetos.

Classificando objetos da Quarentena

Por padrão, objetos na lista de objetos na Quarentena são classificados por data de colocação na Quarentena em ordem cronológica inversa. Para localizar o objeto requerido, é possível classificar os objetos pelas colunas com informações sobre eles. Os resultados classificados serão salvos caso você feche e abra novamente o node **Quarentena** ou feche o Console do Aplicativo, salve o arquivo msc e, em seguida, abra-o novamente a partir desse arquivo.

Para classificar objetos:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Selecione o node secundário **Quarentena**.

3. No painel de resultados do node **Quarentena**, selecione o título da coluna que deseja utilizar para classificar os objetos na lista.

Os objetos na lista serão classificados com base na configuração selecionada.

Filtrando objetos da Quarentena

Para localizar o objeto requerido da quarentena, é possível filtrar objetos da lista, ou seja, exibir apenas os objetos que atendem aos critérios de filtragem (filtros) especificados. Os resultados filtrados serão salvos caso você feche e abra novamente o node **Quarentena** ou feche o Console do Aplicativo, salve o arquivo msc e, em seguida, abra-o novamente a partir desse arquivo.

Para especificar um ou mais filtros:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Selecione o node secundário **Quarentena**.
3. Selecione **Filtrar** no menu de contexto do nome do node.

   A janela **Configurações de filtro** é exibida.
4. Para adicionar um filtro, execute os passos que se seguem:
   a. Na lista **Nome do campo**, selecione o campo que será a base do filtro.
   b. Na lista **Operador**, selecione a condição de filtragem. As condições de filtragem na lista podem ser diferentes dependendo do valor que você selecionou na lista **Nome do campo**.
   c. Insira o valor do filtro no campo **Valor do campo** ou selecione um valor de filtro.
   d. Clique no botão **Adicionar**.

   O filtro adicionado será exibido na lista de filtros na janela **Configurações de filtro**. Repita as etapas de a-d para cada filtro adicionado. Siga estas diretrizes ao trabalhar com filtros:

   - Para combinar vários filtros usando o operador lógico "AND", selecione **Se todas as condições forem atendidas**.
   - Para combinar vários filtros usando o operador lógico "OR", selecione **Se alguma condição for atendida**.
   - Para excluir um filtro, selecione o filtro que deseja excluir na lista de filtros e clique no botão **Remover**.
   - Para editar um filtro, selecione o filtro na lista, na janela **Configurações de filtro**. Em seguida, altere os valores requeridos nos campos **Nome do campo**, **Operador** ou **Valor do campo** e clique no botão **Substituir**.
5. Após todos os filtros serem adicionados, clique no botão **Aplicar**.

Os filtros criados serão salvos.

Para voltar a exibir todos os objetos em Quarentena,

selecione **Quarentena** no menu de contexto do node **Remover filtro**.

Verificação da Quarentena

Por padrão, após cada atualização do banco de dados, o Kaspersky Embedded Systems Security for Windows executa a tarefa local do sistema de Verificação da quarentena. As configurações da tarefa estão descritas na tabela a seguir. As configurações da tarefa de Verificação da Quarentena não podem ser modificadas.

É possível configurar a programação de inicialização da tarefa, iniciá-la manualmente e modificar as permissões da conta usada para iniciar a tarefa.

Após verificar objetos da Quarentena depois de uma atualização do banco de dados, o Kaspersky Embedded Systems Security for Windows poderá reclassificar alguns dos objetos como não infectados: o status desses objetos muda para **Alarme falso**. Outros objetos podem ser reclassificados como infectados e, nesse caso, o Kaspersky Embedded Systems Security for Windows os trata como especificados pela Verificação da Quarentena: desinfecta ou exclui se a desinfecção falhar.

Configurações da tarefa de Verificação da Quarentena

Configuração da tarefa de Verificação da Quarentena	Valor
Escopo da verificação.	Pasta da Quarentena
Configurações de segurança.	O mesmo para todo o escopo da verificação; os valores são fornecidos na tabela a seguir

Configurações de verificação na tarefa de Verificação da quarentena

Configuração de segurança	Valor
Verificar objetos	Todos os objetos incluídos no escopo da verificação
Desempenho	Desativado
Ação a ser executada em objetos infectados e outros	Desinfectar; excluir se a desinfecção não for possível
Ação a ser executada em objetos possivelmente infectados	Ignorar
Excluir arquivos	Não
Não detectar	Não
Parar a verificação se demorar mais que (s)	Não definido
Não verificar objetos com mais de (MB)	Não definido
Verificar fluxos NTFS alternativos	Ativado
Verificar setores de inicialização do disco e MBR	Desativado
Usar a tecnologia iChecker	Desativado
Usar a tecnologia iSwift	Desativado
Verificar objetos compostos	• **Arquivos compactados*** • **Arquivos compactados SFX*** • **Objetos compactados***

	• **Objetos OLE inseridos*** * A opção **Verificar apenas arquivos novos e modificados** está desativada.
Verificar assinatura da Microsoft nos arquivos	Não executado
Usar o analisador heurístico	Ativado com o nível de análise **Profundo**
Zona Confiável	Não aplicado

Restaurando objetos da Quarentena

O Kaspersky Embedded Systems Security for Windows coloca objetos possivelmente infectados na pasta da Quarentena em um formato criptografado para proteger o dispositivo protegido contra qualquer possível efeito negativo.

É possível restaurar qualquer objeto da Quarentena. Isso poderá ser necessário nos seguintes casos:

- Após a Verificação da quarentena usando o banco de dados atualizado, o status do objeto mudar para **Alarme falso** ou **Desinfectado**.
- Você considerar o objeto inofensivo para o dispositivo protegido e desejar utilizá-lo. Caso não deseje que o Kaspersky Embedded Systems Security for Windows isole o objeto durante as verificações subsequentes, você poderá excluí-lo do processamento na tarefa de Proteção de Arquivos em Tempo Real e nas tarefas de Verificação por Demanda. Para isso, especifique o objeto nas configurações de segurança **Excluir arquivos** (pelo nome do arquivo) ou **Não detectar** das tarefas, ou adicione-o à Zona Confiável.

Ao restaurar objetos, é possível selecionar onde o objeto restaurado será salvo: no local original (padrão), em uma pasta especial para objetos restaurados no dispositivo protegido ou em uma pasta personalizada no dispositivo protegido no qual o Console do Aplicativo esteja instalado, ou ainda num dispositivo diferente da rede.

Você pode especificar a pasta para o armazenamento de objetos restaurados no dispositivo protegido. Você pode definir configurações especiais de segurança para que ela seja verificada. O caminho dessa pasta é definido pelas configurações da Quarentena.

A restauração de objetos da Quarentena pode levar à infecção do dispositivo protegido.

É possível restaurar o objeto e salvar uma cópia dele na pasta da Quarentena para usá-la posteriormente, por exemplo, para verificar novamente o objeto após o banco de dados ser atualizado.

Caso um objeto em quarentena esteja contido em um objeto composto (por exemplo, em um arquivo compactado), o Kaspersky Embedded Systems Security for Windows não incluirá o objeto em quarentena ao restaurar o objeto composto. Um objeto em quarentena é salvo separadamente na pasta selecionada.

É possível restaurar um ou mais objetos.

Para restaurar objetos colocados na quarentena, execute os passos a seguir:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Selecione o node secundário **Quarentena**.

3. Execute uma das ações a seguir no painel de detalhes do nó **Quarentena**:

   - Para restaurar um objeto, selecione **Restaurar** no menu de contexto do objeto que deseja restaurar.
   - Para restaurar vários objetos, selecione os objetos que você deseja restaurar usando a tecla **Ctrl** ou **Shift**, clique com o botão direito do mouse em um dos objetos selecionados e selecione **Restaurar** no menu de contexto.

   A janela **Restauração de objeto** é exibida.

4. Na janela **Restauração de objeto**, especifique a pasta em que o objeto restaurado será salvo para cada objeto selecionado.

   O nome do objeto é exibido no campo **Objeto** na parte superior da janela. Se você selecionar vários objetos, o nome do primeiro objeto na lista de objetos selecionados será exibido.

5. Execute uma das seguintes ações:

   - Para restaurar um objeto em seu local original, selecione **Restaurar na pasta de origem**.
   - Para restaurar um objeto na pasta especificada como a localização para objetos restaurados nas configurações, selecione**Restaurar na pasta padrão para restauração**.
   - Para salvar um objeto em uma pasta diferente do dispositivo protegido no qual o Console do Aplicativo esteja instalado, selecione **Restaurar na pasta em seu computador local** e, em seguida, selecione a pasta desejada ou especifique o caminho para ela.

6. Caso deseje salvar uma cópia na pasta de *Quarentena* após restaurar o objeto, desmarque a caixa de seleção **Remover objetos do armazenamento depois que forem restaurados**.

7. Para aplicar as condições de restauração especificadas ao resto dos objetos selecionados, marque a caixa **Aplicar a todos os objetos selecionados**.

   Todos os objetos selecionados são restaurados e salvos no local especificado. Se você selecionou **Restaurar na pasta de origem**, cada um dos objetos será salvo em sua localização original; se você selecionou **Restaurar na pasta padrão para restauração** ou **Restaurar na pasta em seu computador local**, todos os objetos serão salvos na pasta especificada.

8. Clique no botão **OK**.

   O Kaspersky Embedded Systems Security for Windows começará a restaurar o primeiro dos objetos selecionados.

9. Se um objeto com esse nome já existir na localização especificada, a janela **Já existe um objeto com este nome** é exibida.

   a. Selecione uma das seguintes ações para o Kaspersky Embedded Systems Security for Windows:

      - **Substituir**, para substituir o objeto existente pelo objeto restaurado.
      - **Renomear**, para salvar um objeto restaurado com outro nome. No campo de entrada, insira o novo nome de arquivo e caminho completo do objeto restaurado.
      - **Renomear adicionando um sufixo**, para renomear o objeto restaurado adicionando um sufixo ao seu nome de arquivo. Insira o sufixo no campo de entrada.

b. Caso tenha selecionado vários objetos para restauração, selecione a caixa **Renomear** para aplicar a ação selecionada (**Aplicar a todos os objetos selecionados** ou **Substituir**) ao resto dos objetos selecionados. Caso você tenha selecionado **Renomear**, a caixa de seleção **Aplicar a todos os objetos selecionados** estará indisponível.

c. Clique no botão **OK**.

O objeto será restaurado. As informações sobre a operação de restauração serão registradas no log de auditoria do sistema.

Caso você não tenha selecionado a opção **Aplicar a todos os objetos selecionados** na janela **Restauração de objeto**, a janela **Restauração de objeto** poderá ser aberta novamente. Use essa janela para especificar a localização onde o próximo objeto selecionado será salvo (consulte a Etapa 4 desse procedimento).

Movimentação de objetos para a Quarentena

Você pode colocar arquivos na Quarentena manualmente.

Para colocar um arquivo em Quarentena:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Quarentena**.
2. Selecione **Adicionar**.
3. Na janela **Abrir**, selecione o arquivo no disco que deseja colocar na Quarentena.
4. Clique no botão **OK**.

O Kaspersky Embedded Systems Security for Windows isolará em quarentena o arquivo selecionado.

Excluindo objetos da Quarentena

Com base nas configurações da tarefa de Verificação da Quarentena, o Kaspersky Embedded Systems Security for Windows exclui automaticamente objetos da pasta de Quarentena caso seu status tenha sido alterado para *Infectado* durante a Verificação da Quarentena com bancos de dados atualizados e caso o Kaspersky Embedded Systems Security for Windows não tenha conseguido desinfectá-los. O Kaspersky Embedded Systems Security for Windows não remove outros objetos da Quarentena.

É possível excluir um ou mais objetos da Quarentena.

Para excluir um ou mais objetos da Quarentena:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Selecione o node secundário **Quarentena**.
3. Execute uma das seguintes ações:

- Para remover um objeto, selecione **Remover** no menu de contexto do nome do objeto.
- Para excluir vários objetos, selecione os objetos que deseja excluir usando a tecla **Ctrl** ou **Shift**, abra o menu de contexto em um dos objetos selecionados e marque **Remover**.

4. Na janela de confirmação, clique no botão **Sim** para confirmar a operação.

Os objetos selecionados serão removidos da Quarentena.

Envio de objetos possivelmente infectados à Kaspersky para análise

Se o comportamento de um arquivo der um motivo para suspeitar que ele contém uma ameaça, e se o Kaspersky Embedded Systems Security for Windows considerar o arquivo como limpo, você pode ter encontrado uma ameaça desconhecida cuja assinatura ainda não foi adicionada ao banco de dados. É possível enviar esse arquivo à Kaspersky para análise. Os analistas de Antivírus da Kaspersky o examinarão e, se detectada uma nova ameaça, será adicionado um registro aos bancos de dados identificando-a. Ao verificar o objeto novamente após a atualização do banco de dados, é provável que o Kaspersky Embedded Systems Security for Windows identifique o objeto como infectado e possa desinfectá-lo. Além de poder manter o objeto, você também evitará um surto de vírus.

Somente os arquivos da Quarentena podem ser enviados para análise. Os arquivos da Quarentena são armazenados em forma criptografada e não são excluídos pelo aplicativo Antivírus instalado no servidor de e-mail ao serem enviados.

Um objeto em Quarentena não poderá ser enviado à Kaspersky para análise depois que a licença expirar.

Para enviar um arquivo para análise da Kaspersky:

1. Se o arquivo não foi adicionado à Quarentena, comece movendo-o para a **Quarentena**.

2. No node **Quarentena**, abra o menu de contexto do arquivo que deseja enviar para análise e selecione **Enviar objeto para análise**.

3. Na janela de confirmação exibida, clique em **Sim** se estiver seguro que deseja enviar o objeto selecionado para a análise.

4. Se houver um programa de e-mail configurado no dispositivo protegido em que o Console do Aplicativo está instalado, uma nova mensagem de e-mail será criada. Revise-a e clique no botão **Enviar**.

   O campo **Destinatário** conterá o endereço de e-mail da Kaspersky, newvirus@kaspersky.com. O campo Assunto conterá o texto "Quarantined object".

   O corpo da mensagem conterá o seguinte texto: “Este arquivo será enviado à Kaspersky para análise.” Qualquer informação adicional sobre o arquivo, o motivo pelo qual foi considerado possivelmente infectado ou perigoso, como se comportou ou como afeta o sistema pode ser incluído no corpo da mensagem.

   Um arquivo compactado com o nome <Nome do objeto>.cab será anexado à mensagem. Este arquivo comprimido conterá um arquivo <uuid>.klq com o objeto em formato criptografado, um arquivo <uuid>.txt com informações sobre o objeto recebidas do Kaspersky Embedded Systems Security for Windows, além de um arquivo Sysinfo.txt, que contém as seguintes informações sobre o Kaspersky Embedded Systems Security for Windows e o sistema operacional instalado no dispositivo protegido:

   - Nome e versão do sistema operacional.
   - Nome e versão do Kaspersky Embedded Systems Security for Windows.
   - Data de lançamento da atualização do banco de dados mais recente instalada.
   - Chave ativa.

Essas informações são necessárias para que os analistas de Antivírus da Kaspersky examinem seu arquivo de forma mais rápida e eficiente. No entanto, caso não deseje enviar essas informações, você poderá excluir o arquivo Sysinfo.txt do arquivo comprimido.

Se um programa de e-mail não estiver instalado no dispositivo protegido com o Console do Aplicativo, o aplicativo solicitará que o objeto criptografado selecionado seja salvo no arquivo. Esse arquivo pode ser enviado à Kaspersky manualmente.

Para salvar um objeto criptografado em um arquivo:

1. Na janela aberta com uma solicitação para salvar o objeto, clique em **OK**.
2. Selecione uma pasta na unidade do dispositivo protegido ou uma pasta de rede na qual deseja salvar o arquivo que contém o objeto.

O objeto será salvo em um arquivo CAB.

Configurando a Quarentena

É possível definir as configurações da Quarentena. As novas configurações da Quarentena são aplicadas imediatamente após salvar.

Para definir as configurações de Quarentena:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Abra o menu de contexto do node secundário **Quarentena**.
3. Selecione **Propriedades**.
4. Na **Quarentena**: na janela **Propriedades**, defina as configurações da Quarentena necessárias de acordo com seus requisitos:
   - Na seção **Configurações da Quarentena**:
     - Pasta da Quarentena
     - Tamanho máximo da Quarentena (MB)
     - Valor limite de espaço disponível (MB)

     Se o tamanho dos objetos na Quarentena exceder o tamanho de máximo da Quarentena ou exceder o limite de espaço disponível, o Kaspersky Embedded Systems Security for Windows o notificará sobre isto enquanto continua colocando objetos na Quarentena.
   - Na seção **Configurações de restauração**:
     - Pasta destino para a restauração de objetos
5. Clique no botão **OK**.

As configurações de Quarentena recém-definidas serão salvas.

Estatísticas da Quarentena

É possível exibir informações sobre o número de objetos da Quarentena, ou seja, as estatísticas da Quarentena.

Para exibir as estatísticas da Quarentena,

abra o menu de contexto do node **Quarentena** na árvore do Console do Aplicativo e selecione **Estatísticas**.

A janela **Estatísticas da quarentena** exibe informações sobre o número de objetos atualmente armazenados na Quarentena (consulte a tabela seguinte):

Campo	Descrição
Objetos possivelmente infectados	Número de objetos encontrados pelo Kaspersky Embedded Systems Security for Windows que estão possivelmente infectados.
Espaço usado da quarentena	Quantidade total de dados na pasta da Quarentena.
Falsos positivos	O número de objetos que receberam o status de *Alarme falso* porque foram classificados como não infectados durante uma Verificação da Quarentena usando bancos de dados atualizados.
Objetos desinfectados	O número de objetos que receberam o status *Desinfectado* após a Verificação da Quarentena.
Número total de objetos	Número total de objetos na Quarentena.

Como fazer cópias de backup de objetos. Backup

Essa seção fornece informações sobre o backup de objetos maliciosos detectados antes da desinfecção ou exclusão, bem como instruções para a configuração do Backup.

Sobre o backup de objetos antes da desinfecção ou exclusão

O Kaspersky Embedded Systems Security for Windows armazena cópias criptografadas de objetos classificados como *Infectados* no *Backup* antes de desinfectá-los ou excluí-los.

Se o objeto fizer parte de um objeto composto (por exemplo, parte de um arquivo compactado), o Kaspersky Embedded Systems Security for Windows salvará o objeto composto inteiro no Backup. Por exemplo, se o Kaspersky Embedded Systems Security for Windows tiver detectado que um dos objetos de um banco de dados de e-mail está infectado, ele fará backup de todo o banco de dados de e-mail.

Objetos grandes colocados no Backup pelo Kaspersky Embedded Systems Security for Windows podem tornar o sistema lento e reduzir o espaço disponível no disco rígido.

É possível restaurar arquivos do Backup para sua pasta original ou para outra pasta do dispositivo protegido ou de outro dispositivo na rede local. Um arquivo pode ser restaurado do Backup, por exemplo, se um arquivo infectado contiver informações importantes, mas o Kaspersky Embedded Systems Security for Windows não consegue desinfectá-lo sem danificar sua integridade e perder as informações.

A restauração de arquivos do Backup pode levar à infecção do dispositivo protegido.

Visualizando objetos armazenados no Backup

Os objetos podem ser visualizados na pasta do Backup somente usando o Console do Aplicativo no node **Backup**. Não é possível exibi-los usando os gerenciadores de arquivos do Microsoft Windows.

Para visualizar os objetos do Backup,

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Selecione o node secundário **Backup**.

   As informações sobre objetos colocados no Backup são exibidas no painel de resultados do node selecionado.

Para encontrar o objeto necessário na lista de objetos no Backup,

classifique os objetos ou filtre os objetos.

Classificando arquivos no Backup

Por padrão, os arquivos no Backup são classificados pela data do backup em ordem cronológica inversa. Para localizar o arquivo requerido, é possível ordenar os arquivos de acordo com o conteúdo de qualquer coluna no painel de resultados.

Os resultados da classificação serão salvos caso você feche e abra novamente o node **Backup** ou feche o Console do Aplicativo, salve o arquivo msc e, em seguida, abra-o novamente a partir desse arquivo.

Para classificar os arquivos no Backup:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Selecione o node secundário **Backup**.
3. Na lista de arquivos no nó **Backup**, selecione o cabeçalho da coluna que deseja usar para classificar os objetos.

   Os arquivos no Backup serão classificados com base no critério selecionado.

Filtrando arquivos no Backup

Para localizar o arquivo requerido no backup, é possível filtrar os arquivos: exibir no node **Backup** apenas os arquivos que atendam aos critérios de filtragem especificados (filtros).

Os resultados da classificação serão salvos caso você feche e abra novamente o node **Backup** ou feche o Console do Aplicativo, salve o arquivo msc e, em seguida, abra-o novamente a partir desse arquivo.

Para filtrar os arquivos no Backup:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Backup** e selecione **Filtrar**.

   A janela **Configurações de filtro** é exibida.

2. Para adicionar um filtro, execute os passos que se seguem:

   a. Na lista **Nome do campo**, selecione o campo que será a base do filtro.

   b. Na lista **Operador**, selecione a condição de filtragem. As condições de filtragem na lista podem ser diferentes dependendo do valor que você selecionou no campo **Nome do campo**.

   c. Insira o valor do filtro no campo **Valor do campo** ou selecione um valor de filtro.

   d. Clique no botão **Adicionar**.

   O filtro adicionado será exibido na lista de filtros na janela **Configurações de filtro**. Repita essas etapas para cada filtro adicionado. Siga estas diretrizes ao trabalhar com filtros:

   - Para combinar vários filtros usando o operador lógico "AND", selecione **Se todas as condições forem atendidas**.
   - Para combinar vários filtros usando o operador lógico "OR", selecione **Se alguma condição for atendida**.
   - Para excluir um filtro, selecione o filtro que deseja excluir na lista de filtros e clique no botão **Remover**.
   - Para editar o filtro, selecione-o na lista de filtros na janela **Configurações de filtro**, modifique os valores necessários nos campos **Nome do campo**, **Operador** e **Valor do campo**, e clique no botão **Substituir**.

   Quando todos os filtros tiverem sido adicionados, clique no botão **Aplicar**. Somente arquivos correspondentes aos filtros especificados serão exibidos na lista.

Para exibir todos os arquivos incluídos na lista de objetos armazenados no Backup,

selecione **Backup** no menu de contexto do node **Remover filtro**.

Restaurando arquivos do Backup

O Kaspersky Embedded Systems Security for Windows armazena arquivos na pasta Backup em formato criptografado para proteger o dispositivo protegido contra seus possíveis efeitos prejudiciais.

Qualquer arquivo pode ser restaurado do Backup.

Talvez seja necessário restaurar um arquivo nos seguintes casos:

- O arquivo infectado original continha informações importantes e o Kaspersky Embedded Systems Security for Windows não conseguiu manter a sua integridade; como resultado, as informações no arquivo ficaram indisponíveis.
- Você considera o arquivo inofensivo para o dispositivo protegido e desejar utilizá-lo. Caso não deseje que o Kaspersky Embedded Systems Security for Windows considere esse arquivo como infectado ou possivelmente infectado, durante verificações subsequentes é possível excluí-lo do processamento na tarefa de Proteção de

Arquivos em Tempo Real e nas tarefas de Verificação por Demanda. Para isso, especifique o arquivo na configuração **Excluir arquivos** ou **Não detectar** nas tarefas correspondentes.

A restauração de arquivos do Backup pode levar à infecção do dispositivo protegido.

Ao restaurar um arquivo, é possível selecionar a localização onde deseja salvá-lo: no local original (padrão), em uma pasta especial para objetos restaurados no dispositivo protegido ou em uma pasta personalizada no dispositivo protegido no qual o Console do Aplicativo está instalado, ou ainda num dispositivo diferente na rede.

Você pode especificar a pasta para o armazenamento de objetos restaurados no dispositivo protegido. Você pode definir configurações especiais de segurança para que ela seja verificada. O caminho para essa pasta é especificado pelas Configurações de Backup.

Por padrão, quando o Kaspersky Embedded Systems Security for Windows restaura um arquivo, ele faz uma cópia desse arquivo no Backup. A cópia do arquivo pode ser excluída do Backup depois de ser restaurada.

Para restaurar os arquivos do Backup:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Selecione o node secundário **Backup**.
3. Execute uma das ações a seguir no painel de detalhes do nó **Backup**:
   - Para restaurar um objeto, selecione **Restaurar** no menu de contexto do objeto que deseja restaurar.
   - Para restaurar vários objetos, selecione os objetos que você deseja restaurar usando a tecla **Ctrl** ou **Shift**, clique com o botão direito do mouse em um dos objetos selecionados e selecione **Restaurar** no menu de contexto.

   A janela **Restauração de objeto** é exibida.
4. Na janela **Restauração de objeto**, especifique a pasta em que o objeto restaurado será salvo para cada objeto selecionado.

   O nome do objeto é exibido no campo **Objeto** na parte superior da janela. Se você selecionar vários objetos, o nome do primeiro objeto na lista de objetos selecionados será exibido.
5. Execute uma das seguintes ações:
   - Para restaurar um objeto em seu local original, selecione **Restaurar na pasta de origem**.
   - Para restaurar um objeto na pasta especificada como a localização para objetos restaurados nas configurações, selecione**Restaurar na pasta padrão para restauração**.
   - Para salvar um objeto em uma pasta diferente do dispositivo protegido no qual o Console do Aplicativo esteja instalado, selecione **Restaurar na pasta em seu computador local** e, em seguida, selecione a pasta desejada ou especifique o caminho para ela.
6. Caso deseje salvar uma cópia do arquivo na pasta do Backup após ele ser restaurado, marque a caixa de seleção **Remover objetos do armazenamento depois que forem restaurados** (por padrão, esta caixa é desmarcada).

7. Para aplicar as condições de restauração especificadas ao resto dos objetos selecionados, marque a caixa **Aplicar a todos os objetos selecionados**.

   Todos os objetos selecionados são restaurados e salvos no local especificado. Se você selecionou **Restaurar na pasta de origem**, cada um dos objetos será salvo em sua localização original; se você selecionou **Restaurar na pasta padrão para restauração** ou **Restaurar na pasta em seu computador local**, todos os objetos serão salvos na pasta especificada.

8. Clique no botão **OK**.

   O Kaspersky Embedded Systems Security for Windows começará a restaurar o primeiro dos objetos selecionados.

9. Se um objeto com esse nome já existir na localização especificada, a janela **Já existe um objeto com este nome** é exibida.

   a. Selecione uma das seguintes ações para o Kaspersky Embedded Systems Security for Windows:

   - **Substituir**, para substituir o objeto existente pelo objeto restaurado.
   - **Renomear**, para salvar um objeto restaurado com outro nome. No campo de entrada, insira o novo nome de arquivo e caminho completo do objeto restaurado.
   - **Renomear adicionando um sufixo**, para renomear o objeto restaurado adicionando um sufixo ao seu nome de arquivo. Insira o sufixo no campo de entrada.

   b. Caso tenha selecionado vários objetos para restauração, selecione a caixa **Renomear** para aplicar a ação selecionada (**Aplicar a todos os objetos selecionados** ou **Substituir**) ao resto dos objetos selecionados. Caso você tenha selecionado **Renomear**, a caixa de seleção **Aplicar a todos os objetos selecionados** estará indisponível.

   c. Clique no botão **OK**.

   O objeto será restaurado. As informações sobre a operação de restauração serão registradas no log de auditoria do sistema.

Caso você não tenha selecionado a opção **Aplicar a todos os objetos selecionados** na janela **Restauração de objeto**, a janela **Restauração de objeto** poderá ser aberta novamente. Use essa janela para especificar a localização onde o próximo objeto selecionado será salvo (consulte a Etapa 4 desse procedimento).

Excluindo arquivos do Backup

Para excluir um ou mais arquivos do Backup:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Selecione o node secundário **Backup**.
3. Execute uma das seguintes ações:

   - Para remover um objeto, selecione **Remover** no menu de contexto do nome do objeto.
   - Para excluir vários objetos, selecione os objetos que deseja excluir usando a tecla **Ctrl** ou **Shift**, abra o menu de contexto em um dos objetos selecionados e marque **Remover**.

4. Na janela de confirmação, clique no botão **Sim** para confirmar a operação.

Os arquivos selecionados serão excluídos do Backup.

Configurando o Backup

Para definir as configurações de Backup:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.
2. Abra o menu de contexto no node **Backup**.
3. Selecione **Propriedades**.
4. Em **Backup**: na janela **Propriedades**, defina as configurações de backup necessárias de acordo com seus requisitos:

   Na seção **Configurações de backup**:

   - Pasta de backup
   - Tamanho máximo do backup (MB)
   - Valor limite de espaço disponível (MB)

     > Se o tamanho dos objetos no Backup exceder o tamanho máximo do Backup ou exceder o limite de espaço disponível, o Kaspersky Embedded Systems Security for Windows o notificará sobre isto enquanto continua colocando objetos no Backup.

   Na seção **Configurações de restauração**:

   - Pasta destino para a restauração de objetos
5. Clique no botão **OK**.

As definições de Backup configuradas serão salvas.

Estatísticas do backup

É possível visualizar informações sobre o status atual do Backup, ou seja, estatísticas do backup.

Para exibir as estatísticas do Backup,

abra o menu de contexto do node **Backup** na árvore do Console do Aplicativo e selecione **Estatísticas**. A janela **Estatísticas do backup** é exibida.

A janela **Estatísticas do backup** exibe as informações sobre o status atual do Backup (consulte a tabela abaixo).

Informações sobre o status atual do Backup

Campo	Descrição
Tamanho de Backup atual	Quantidade de dados na pasta de Backup; o aplicativo calcula o tamanho do arquivo em formato criptografado

Número total de objetos	Número atual total de objetos no Backup

Bloqueio do acesso aos recursos da rede. Sessões de rede bloqueadas

Esta seção descreve como bloquear dispositivos remotos e definir as configurações da lista de sessões de rede bloqueadas.

Lista de sessões de rede bloqueadas

Por padrão, a lista de sessões de rede bloqueadas está disponível para uso se algum dos seguintes componentes estiver instalado: Proteção de Arquivos em Tempo Real, Proteção Contra Ameaças à Rede. Esses componentes descobrem as tentativas remotas de criptografar, abrir ou executar objetos no dispositivo protegido ou nas pastas compartilhadas de armazenamento conectadas à rede, de acordo com a lista de sessões de rede bloqueadas. As informações sobre as sessões de rede bloqueadas de todos os dispositivos protegidos são enviadas ao Kaspersky Security Center. O Kaspersky Embedded Systems Security for Windows bloqueia a sessão atual e, em termos da sessão atual, torna as pastas compartilhadas ou as pastas de armazenamento anexadas à rede indisponíveis.

A lista de sessões de rede bloqueadas é preenchida quando ao menos uma das seguintes tarefas é iniciada no modo ativo (sob condições específicas):

- Para a tarefa de Proteção de Arquivos em Tempo Real: a atividade maliciosa de um dispositivo que acessa os recursos de arquivos de rede é detectada e, nas configurações da tarefa de Proteção de Arquivos em Tempo Real, a caixa de seleção **Bloquear o acesso a recursos de rede compartilhados para sessões que exibem atividade maliciosa** está marcada.

- Para a tarefa de Proteção Contra Ameaças à Rede: uma atividade típica de ataques à rede é detectada.

Depois que atividade maliciosa ou uma tentativa de criptografia é detectada, a tarefa envia informações sobre a sessão de rede atacante para a Lista de sessões de rede bloqueadas e o aplicativo cria um evento de *Aviso* para a sessão atual do host invasor. Qualquer tentativa desta sessão de acessar as pastas de rede compartilhadas protegidas será bloqueada.

Caso o identificador exclusivo local (LUID) de um host que iniciou o ataque à sessão de rede seja adicionado à Lista de sessões de rede bloqueadas, o Kaspersky Embedded Systems Security for Windows determinará o endereço IP do host e o adicionará à lista de sessões de rede bloqueadas em vez do LUID do host invasor.

Por padrão, o Kaspersky Embedded Systems Security for Windows remove as sessões de rede bloqueadas da lista 30 minutos após serem adicionados. O acesso aos recursos de arquivos de rede é restaurado automaticamente após serem excluídos da lista de sessões de rede bloqueadas. É possível especificar depois de quanto tempo as sessões de rede bloqueadas serão desbloqueadas automaticamente.

Observe que, quando o acesso ao gerenciamento de armazenamento de qualquer conta de usuário é restringido, a lista de sessões de rede bloqueadas ainda estará disponível. As configurações de sessões de rede bloqueadas não podem ser alteradas, a menos que a conta de usuário selecionada tenha **Permissões de edição** para gerenciar o Kaspersky Embedded Systems Security for Windows.

Gerenciamento da lista de sessões de rede bloqueadas usando o plugin de Administração

Nesta seção, saiba como definir as configurações da Lista de sessões de rede bloqueadas por meio da interface do Plug-in de Administração.

Ativação do bloqueio de hosts não confiáveis

Para adicionar sessões de rede que exibem qualquer atividade maliciosa ou de criptografia na **Lista de sessões de rede bloqueadas** e bloquear o acesso aos recursos de arquivos de rede, ao menos uma das tarefas a seguir deve ser executada no modo ativo:

- Proteção de Arquivos em Tempo Real
- Proteção Contra Ameaças à Rede

Configure a tarefa de Proteção de Arquivos em Tempo Real:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados**.
2. Selecione a guia **Políticas** e abra **<Nome da política>** >**Proteção do Computador em Tempo Real** > **Configurações** no bloco **Proteção de Arquivos em Tempo Real**.

   A janela **Proteção do Computador em Tempo Real** é exibida.
3. Na seção **Integração com outros componentes**, marque a caixa de seleção **Listar hosts que exibem atividades maliciosas como não confiáveis** se quiser que o Kaspersky Embedded Systems Security for Windows bloqueie o acesso a recursos de arquivos de rede para hosts nos quais são detectadas atividades maliciosas durante a execução da tarefa de Proteção de Arquivos em Tempo Real.
4. Se a tarefa não for iniciada, abra a guia **Gerenciamento da tarefa**:

   a. Marque a caixa de seleção **Executar de acordo com o agendamento**.

   b. Selecione a frequência para a opção **Ao iniciar o aplicativo** na lista suspensa.
5. Na janela **Proteção do Computador em Tempo Real**, clique em **OK**.

As configurações recém-definidas são salvas.

Configure a tarefa de Proteção Contra Ameaças à Rede:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.

5. Na janela **Propriedades: <Nome da política>**, selecione a seção.

6. Clique no botão **Configurações** na subseção **Proteção Contra Ameaças à Rede**.

   A janela **Proteção Contra Ameaças à Rede** é exibida.

7. Abra a guia **Geral**.

8. Na seção **Modo de processamento** selecione a opção **Bloquear conexões quando um ataque for detectado**.

   A caixa de seleção ativa ou desativa a adição de hosts que exibam uma atividade típica de ataques à rede na lista de hosts bloqueados.

   Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, registrará os eventos sobre a atividade detectada e adicionará os endereços IP de hosts que exibem atividades típicas de ataques à rede na lista de hosts bloqueados.

   Você pode visualizar a lista de hosts bloqueados no Armazenamento de Hosts Bloqueados.

   É possível restaurar o acesso aos hosts bloqueados e especificar quantos dias, horas e minutos depois do bloqueio eles poderão recuperar o acesso aos recursos de arquivos de rede pela definição das configurações de Armazenamento de Hosts Bloqueados.

   O modo é selecionado por padrão.

9. Se a tarefa não for iniciada, abra a guia **Gerenciamento da tarefa**:

   a. Marque a caixa de seleção **Executar de acordo com o agendamento**.

   b. Selecione a frequência para a opção **Ao iniciar o aplicativo** na lista suspensa.

10. Na janela, clique em **OK**.

11. As configurações recém-definidas são salvas.

Definindo as configurações para a lista de sessões de rede bloqueadas

Para configurar a Lista de sessões de rede bloqueadas:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Suplementar**, clique no botão **Configurações** na subseção **Armazenamentos**.

   A janela **Configurações de armazenamentos** é exibida.

5. Na seção **Termos de bloqueio da sessão de rede** da guia **Sessões de rede bloqueadas**, especifique quantos dias, horas e minutos depois do bloqueio as sessões de rede bloqueadas poderão recuperar o acesso aos recursos de arquivos de rede.

6. Clique no botão **OK**.

Gerenciando a lista de sessões de rede bloqueadas por meio do Console do Aplicativo

Nesta seção, saiba como definir as configurações da lista de sessões de rede bloqueadas por meio da interface do Console do Aplicativo.

Ativação do bloqueio de hosts não confiáveis

Para adicionar sessões de rede que exibem qualquer atividade maliciosa ou de criptografia na **Lista de sessões de rede bloqueadas** e bloquear o acesso aos recursos de arquivos de rede, ao menos uma das tarefas a seguir deve ser executada no modo ativo:

- Proteção de Arquivos em Tempo Real
- Proteção Contra Ameaças à Rede

Configure a tarefa de Proteção de Arquivos em Tempo Real:

1. Na árvore do Console do Aplicativo, expanda o node **Proteção do Computador em Tempo Real**.
2. Selecione o node secundário **Proteção de Arquivos em Tempo Real**.
3. Clique no link **Propriedades** no painel de resultados.

   A janela **Configurações de tarefa** é aberta.
4. Na seção **Profundo**, marque a caixa de seleção **Bloquear o acesso a recursos de rede compartilhados para sessões que exibem atividade maliciosa** se desejar que o Kaspersky Embedded Systems Security for Windows bloqueie sessões de rede nas quais são detectadas atividades maliciosas durante a execução da tarefa de Proteção de Arquivos em Tempo Real.
5. Se a tarefa não for iniciada, abra a guia **Agendamento**:
   a. Marque a caixa de seleção **Executar de acordo com o agendamento**.
   b. Selecione a frequência para a opção **Ao iniciar o aplicativo** na lista suspensa.
6. Na janela **Configurações de tarefa** clique em **OK**.

As configurações recém-definidas são salvas.

Configure a tarefa de Proteção Contra Ameaças à Rede:

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.

2. Selecione o nó secundário da **Proteção Contra Ameaças à Rede**.

3. Clique no link **Proteção Contra Ameaças à Rede** no painel de detalhes do nó **Propriedades**.

4. A janela **Configurações de tarefa** é aberta.

5. Abra a guia **Geral**.

6. Na seção **Modo de processamento** selecione a opção **Bloquear conexões quando um ataque for detectado**.

   A caixa de seleção ativa ou desativa a adição de hosts que exibam uma atividade típica de ataques à rede na lista de hosts bloqueados.

   Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, registrará os eventos sobre a atividade detectada e adicionará os endereços IP de hosts que exibem atividades típicas de ataques à rede na lista de hosts bloqueados.

   Você pode visualizar a lista de hosts bloqueados no Armazenamento de Hosts Bloqueados.

   É possível restaurar o acesso aos hosts bloqueados e especificar quantos dias, horas e minutos depois do bloqueio eles poderão recuperar o acesso aos recursos de arquivos de rede pela definição das configurações de Armazenamento de Hosts Bloqueados.

   O modo é selecionado por padrão.

7. Marque ou desmarque a caixa de seleção **Não interromper a análise de tráfego quando a tarefa não estiver em execução**.

   Caso esta caixa de controle esteja selecionada, então, mesmo quando a tarefa de Proteção Contra Ameaças à Rede for interrompida, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede e bloqueará a atividade de rede no computador invasor, dependendo do modo de tarefa selecionado.

   Caso a caixa de seleção esteja desmarcada, quando a tarefa de Proteção Contra Ameaças à Rede for interrompida, o Kaspersky Embedded Systems Security for Windows não verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede.

   Por padrão, a caixa de seleção fica desmarcada.

8. Se a tarefa não for iniciada, abra a guia **Agendamento**:

   a. Marque a caixa de seleção **Executar de acordo com o agendamento**.

   b. Selecione a frequência para a opção **Ao iniciar o aplicativo** na lista suspensa.

9. Na janela **Configurações de tarefa** clique em **OK**.

As configurações recém-definidas são salvas.

Definindo as configurações para a lista de sessões de rede bloqueadas

Para configurar a Lista de sessões de rede bloqueadas:

1. Na árvore do Console do Aplicativo, expanda o node **Armazenamentos**.

2. Abra o menu de contexto do nó secundário **Sessões de rede bloqueadas**.

3. Selecione a opção de menu **Propriedades**.

   A janela **Configurações para a lista de sessões de rede bloqueadas** é exibida.

4. Na seção **Termo de bloqueio da sessão de rede**, especifique quantos dias, horas e minutos depois do bloqueio as sessões de rede bloqueadas poderão recuperar o acesso aos recursos de arquivos de rede.

5. Clique no botão **OK**.

6. Para restaurar o acesso para todas as sessões de rede bloqueadas:

   a. Abra o menu de contexto do nó secundário **Sessões de rede bloqueadas**.

   b. Selecione a opção **Desbloquear todos**.

      Todas as sessões de rede serão removidas da lista e desbloqueadas.

7. Para remover várias sessões de rede da lista de sessões de rede bloqueadas:

   a. Na lista de sessões de rede bloqueadas exibida no painel de resultados, selecione uma ou mais sessões.

   b. Abra o menu de contexto do nó secundário **Sessões de rede bloqueadas**.

   c. Selecione a opção **Desbloquear selecionado**.

      As sessões de rede selecionadas são desbloqueadas.

Gerenciando a lista de sessões de rede bloqueadas por meio do Plugin da Web

Nesta seção, saiba como definir as configurações da lista de sessões de rede bloqueadas por meio da interface do Plug-in da Web.

Ativando o bloqueio de sessões de rede

Para adicionar sessões de rede que exibem qualquer atividade maliciosa ou criptografada na **Sessões de rede bloqueadas** e bloquear o acesso aos recursos de arquivos de rede para essas sessões, ao menos uma das tarefas a seguir deve ser executada no modo ativo:

- Proteção de Arquivos em Tempo Real
- Proteção Contra Ameaças à Rede

Configure a tarefa de Proteção de Arquivos em Tempo Real:

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

2. Clique no nome da política que você quer configurar.

3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.

4. Selecione a seção **Proteção do Computador em Tempo Real**.

5. Clique em **Configurações** na subseção **Proteção de Arquivos em Tempo Real**.

6. Na seção **Integração com outros componentes**, marque a caixa de seleção **Bloquear o acesso a recursos de rede compartilhados para sessões que exibem atividade maliciosa** se desejar que o Kaspersky Embedded Systems Security for Windows bloqueie a sessão atual e torne os recursos compartilhados de rede indisponíveis para as sessões de rede para as quais atividades maliciosas foram detectadas.

7. Se a tarefa não for iniciada, abra a guia **Gerenciamento da tarefa**:

   a. Marque a caixa de seleção **Executar de acordo com o agendamento**.

   b. Selecione a frequência para a opção **Ao iniciar o aplicativo** na lista suspensa.

8. Clique no botão **Salvar**.

As configurações recém-definidas são salvas.

Definindo as configurações para a lista de sessões de rede bloqueadas

Para configurar a Lista de sessões de rede bloqueadas:

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

2. Clique no nome da política que você quer configurar.

3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.

4. Selecione a seção **Suplementar**.

5. Clique no botão **Configurações** na subseção **Armazenamentos**.

6. Na seção **Suplementar**, clique no botão **Configurações** na subseção **Armazenamentos**.

   A janela **Armazenamentos** é exibida.

7. Na seção **Termo de bloqueio da sessão de rede** da guia **Sessões de rede bloqueadas**, especifique quantos dias, horas e minutos depois do bloqueio as sessões de rede bloqueadas poderão recuperar o acesso aos recursos de arquivos de rede.

8. Clique no botão **OK**.

Registro de eventos. Logs do Kaspersky Embedded Systems Security for Windows

Esta seção fornece informações sobre a maneira de trabalhar com os logs do Kaspersky Embedded Systems Security for Windows.

Modos para registrar eventos do Kaspersky Embedded Systems Security for Windows

Os eventos do Kaspersky Embedded Systems Security for Windows são divididos em dois grupos:

- Os eventos relacionados com o processamento de objetos em tarefas do Kaspersky Embedded Systems Security for Windows.
- Os eventos relacionados à administração do Kaspersky Embedded Systems Security for Windows, como a inicialização do aplicativo, criação ou exclusão de tarefas ou edição de configurações da tarefa.

O Kaspersky Embedded Systems Security for Windows usa os seguintes métodos para registrar eventos em log:

- **Logs de tarefas**. Um log de tarefas contém informações sobre o status atual da tarefa e eventos que ocorreram durante sua execução.
- **Log de auditoria do sistema**. O log de auditoria do sistema contém informações sobre eventos relacionados à administração do Kaspersky Embedded Systems Security for Windows.
- **Log de Eventos**. O log de eventos contém informações sobre eventos requeridos para diagnosticar falhas na operação do Kaspersky Embedded Systems Security for Windows. O log de eventos está disponível no Visualizador de Eventos do Microsoft Windows.
- **Log de segurança**. O Log de segurança contém informações sobre eventos associados a violações de segurança ou tentativas de violação de segurança no dispositivo protegido.

Se ocorrer um problema durante a operação do Kaspersky Embedded Systems Security for Windows (por exemplo, se o Kaspersky Embedded Systems Security for Windows ou uma tarefa individual for encerrada de forma anormal ou não for executada), você poderá criar um arquivo de rastreamento e um arquivo de despejo de processos do Kaspersky Embedded Systems Security for Windows e enviar arquivos com essas informações para análise do Suporte Técnico da Kaspersky para diagnosticar o problema encontrado.

O Kaspersky Embedded Systems Security for Windows não envia nenhum arquivo de rastreamento ou de despejo automaticamente. Os dados de diagnóstico só podem ser enviados por um usuário com as permissões necessárias.

O Kaspersky Embedded Systems Security for Windows grava as informações nos arquivos de rastreamento e no arquivo de despejo no formulário 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 for Windows. É possível configurar as permissões de acesso e permitir que apenas os usuários necessários acessem os logs, arquivos de rastreamento e de despejo.

Os arquivos que podem ser baixados pelos links a seguir contêm tabelas com as listas completas de eventos do Kaspersky Embedded Systems Security for Windows das seguintes categorias:

- Eventos que o Kaspersky Embedded Systems Security for Windows grava no log de eventos.

  BAIXAR KESS-WEL-EVENTS.ZIP

- Eventos que o Kaspersky Embedded Systems Security for Windows envia ao Servidor de Administração.

  BAIXAR KESS-KSC-EVENTS.ZIP

Log de auditoria do sistema

O Kaspersky Embedded Systems Security for Windows executa uma auditoria de sistema de eventos relacionados à administração do Kaspersky Embedded Systems Security for Windows. O aplicativo registra informações sobre o início do aplicativo, os inícios e interrupções de tarefas do Kaspersky Embedded Systems Security for Windows, alterações nas configurações da tarefa, criação e exclusão de tarefas de Verificação por Demanda. Os registros desses eventos são exibidos no painel de resultados ao selecionar o node **Log de auditoria do sistema** no Console do Aplicativo.

Por padrão, o Kaspersky Embedded Systems Security for Windows armazena registros no log de auditoria do sistema durante um período ilimitado de tempo. É possível especificar o período de armazenamento para registros no log de auditoria do sistema.

É possível especificar uma pasta que será usada pelo Kaspersky Embedded Systems Security for Windows para armazenar arquivos contendo o log de auditoria do sistema diferentes da pasta padrão.

Classificando eventos no log de auditoria do sistema

Por padrão, os eventos no node Log de auditoria do sistema são exibidos em ordem cronológica inversa.

Os eventos podem ser classificados de acordo com o conteúdo de qualquer coluna, exceto da coluna **Evento**.

Para classificar eventos no log de auditoria do sistema:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.
2. Selecione o node secundário **Log de auditoria do sistema**.
3. No painel de resultados, selecione o título da coluna que deseja utilizar para classificar os eventos na lista.

Os resultados classificados serão salvos para a próxima vez que você visualizar o log de auditoria do sistema.

Filtrando eventos no log de auditoria do sistema

É possível configurar o log de auditoria do sistema para exibir somente os registros de eventos que satisfaçam as condições de filtragem (filtros) especificados.

Para filtrar os eventos no log de auditoria do sistema:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.

2. Abra o menu de contexto do node secundário **Log de auditoria do sistema** e selecione **Filtrar**.

   A janela **Configurações de filtro** é exibida.

3. Para adicionar um filtro, execute os passos que se seguem:

   a. Na lista **Nome do campo**, selecione a coluna que deseja usar para filtrar os eventos.

   b. Na lista **Operador**, selecione a condição de filtragem. As condições de filtragem variam dependendo do item selecionado na lista **Nome do campo**.

   c. Na lista **Valor do campo**, selecione um valor para o filtro.

   d. Clique no botão **Adicionar**.

   O filtro adicionado será exibido na lista de filtros na janela **Configurações de filtro**.

4. Se necessário, execute uma das seguintes ações:

   - Para combinar vários filtros usando o operador lógico "AND", selecione **Se todas as condições forem atendidas**.
   - Para combinar vários filtros usando o operador lógico "OR", selecione **Se alguma condição for atendida**.

5. Clique no botão **Aplicar** para salvar as condições de filtragem no log de auditoria do sistema.

   A lista de eventos do log de auditoria do sistema exibe somente os eventos que atendem às condições do filtro. Os resultados filtrados serão salvos para a próxima vez que você visualizar o log de auditoria do sistema.

Para desativar o filtro:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.

2. Abra o menu de contexto do node secundário **Log de auditoria do sistema** e selecione **Remover filtro**.

   A lista de eventos do log de auditoria do sistema exibirá, então, todos os eventos.

Excluir eventos do Log de auditoria do sistema

Por padrão, o Kaspersky Embedded Systems Security for Windows armazena registros no log de auditoria do sistema durante um período ilimitado de tempo. É possível especificar o período de armazenamento para registros no log de auditoria do sistema.

É possível excluir manualmente todos os eventos do log de auditoria do sistema.

Para excluir eventos do log de auditoria do sistema:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.

2. Abra o menu de contexto do node secundário **Log de auditoria do sistema** e selecione **Limpar**.

3. Execute uma das seguintes ações:

   - Caso queira salvar o conteúdo do log em um arquivo no formato CSV ou TXT antes de excluir os eventos do log de auditoria do sistema, clique no botão **Sim** na janela que solicita a confirmação da exclusão. Na janela que é exibida, especifique o nome e a localização do arquivo.

- Se não quiser salvar o conteúdo do registro em um arquivo, clique no botão **Não** na janela que solicita a confirmação da exclusão.

O log de auditoria do sistema será limpo.

Logs de tarefas

Esta seção fornece informações sobre logs de tarefas do Kaspersky Embedded Systems Security for Windows e instruções sobre como gerenciá-los.

Sobre os Logs de tarefas

As informações sobre a execução de tarefas do Kaspersky Embedded Systems Security for Windows são exibidas no painel de resultados ao selecionar o node **Logs de tarefas** no Console do Aplicativo.

No log de cada tarefa, é possível visualizar as estatísticas de execução da tarefa, os detalhes de cada objeto processado pelo aplicativo desde o início da tarefa e as configurações da tarefa.

Por padrão, o Kaspersky Embedded Systems Security for Windows armazena registros em logs de tarefas por 30 dias após a conclusão da tarefa. Você pode alterar o período de armazenamento de registros em Logs de tarefas.

Você pode especificar uma pasta que será usada pelo Kaspersky Embedded Systems Security for Windows para armazenar os arquivos que contêm os logs de tarefas diferente da pasta padrão. Também é possível selecionar eventos que o Kaspersky Embedded Systems Security for Windows registrará nos logs de tarefas.

Visualizando a lista de eventos em Logs de tarefas

Para exibir os logs de tarefas:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.
2. Selecione o subnó **Logs de tarefas**.

   A lista de eventos salvos em logs de tarefas do Kaspersky Embedded Systems Security for Windows será exibida no painel de resultados.

Os eventos podem ser classificados ou filtrados por qualquer outra coluna.

Classificando logs de tarefas

Por padrão, os logs de tarefas são exibidos por ordem cronológica inversa. Eles podem ser classificados por qualquer coluna.

Para classificar logs de tarefas:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.
2. Selecione o subnó **Logs de tarefas**.

3. No painel de resultados, selecione o título da coluna que deseja utilizar para classificar os logs de tarefas do Kaspersky Embedded Systems Security for Windows.

Os resultados classificados serão salvos para a próxima vez que você visualizar o log de tarefas.

Filtrando logs de tarefas

Você pode configurar a lista de Logs de tarefas para que exiba somente os logs de tarefas que correspondem às condições de filtragem (filtros) que você especificou.

Para filtrar logs de tarefas:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.
2. Abra o menu de contexto do node secundário **Logs de tarefas** e selecione **Filtrar**.

   A janela **Configurações de filtro** é exibida.
3. Para adicionar um filtro, execute os passos que se seguem:

   a. Na lista **Nome do campo**, selecione a coluna que deseja usar para filtrar os logs de tarefas.

   b. Na lista **Operador**, selecione a condição de filtragem. As condições de filtragem variam dependendo do item selecionado na lista **Nome do campo**.

   c. Na lista **Valor do campo**, selecione um valor para o filtro.

   d. Clique no botão **Adicionar**.

   O filtro adicionado será exibido na lista de filtros na janela **Configurações de filtro**.
4. Se necessário, execute uma das seguintes ações:

   - Para combinar vários filtros usando o operador lógico "AND", selecione **Se todas as condições forem atendidas**.
   - Para combinar vários filtros usando o operador lógico "OR", selecione **Se alguma condição for atendida**.
5. Clique no botão **Aplicar** para salvar as condições de filtragem na lista de logs de tarefas.

A lista de logs de tarefas exibe somente os logs de tarefa que atendem às condições do filtro. Os resultados filtrados serão salvos para a próxima vez que você visualizar o log de tarefas.

Para desativar o filtro:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.
2. Abra o menu de contexto do node secundário **Logs de tarefas** e selecione **Remover filtro**.

A lista de logs de tarefas exibirá então todos os eventos.

Visualizando estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security for Windows em logs de tarefas

Nos logs de tarefas, você pode visualizar informações detalhadas sobre todos os eventos que ocorreram nas tarefas desde que foram iniciadas, bem como estatísticas de execução da tarefa e configurações da tarefa.

Para visualizar estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security for Windows:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.
2. Selecione o subnó **Logs de tarefas**.
3. No painel de resultados, abra a janela **Logs** usando um dos seguintes métodos:
   - Clique duas vezes no log de tarefas que deseja visualizar.
   - Abra o menu de contexto do log de tarefas que deseja visualizar e selecione **Exibir registro**.
4. Na janela aberta, são exibidos os seguintes detalhes:
   - A guia **Estatísticas** exibe a hora de início e conclusão da tarefa, bem como as suas estatísticas.
   - A guia **Eventos** exibe uma lista de eventos registrados durante a execução da tarefa.
   - A guia **Opções** exibe as configurações da tarefa.
5. Se necessário, clique no botão **Filtrar** para filtrar os eventos no log de tarefas.
6. Se necessário, clique no botão **Exportar** para exportar dados do log de tarefas para um arquivo em formato CSV ou TXT.
7. Clique no botão **Fechar**.

   A janela **Logs** será fechada.

Exportando informações de um Log de tarefas

Você pode exportar dados de um log de tarefas para um arquivo em formato CSV ou TXT.

Para exportar dados de um log de tarefas:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.
2. Selecione o subnó **Logs de tarefas**.
3. No painel de resultados, abra a janela **Logs** usando um dos seguintes métodos:
   - Clique duas vezes no log de tarefas que deseja visualizar.
   - Abra o menu de contexto do log de tarefas que deseja visualizar e selecione **Exibir registro**.
4. Na parte inferior da janela **Logs**, clique no botão **Exportar**.

   A janela **Salvar como** é exibida.
5. Especifique o nome, a localização, o tipo e a codificação do arquivo para o qual deseja exportar dados do log de tarefas.

6. Clique no botão **Salvar**.

As configurações especificadas são salvas.

Excluindo logs de tarefas

Por padrão, o Kaspersky Embedded Systems Security for Windows armazena registros em logs de tarefas por 30 dias após a conclusão da tarefa. Você pode alterar o período de armazenamento de registros em Logs de tarefas.

Você pode excluir manualmente os logs de tarefas que já foram concluídos.

Eventos dos logs de tarefas em execução e tarefas usadas por outros usuários não serão excluídos.

Para excluir os logs de tarefas:

1. Na árvore do Console do Aplicativo, expanda o node **Logs e notificações**.
2. Selecione o subnó **Logs de tarefas**.
3. Execute uma das seguintes ações:
   - Caso deseje excluir os logs de todas as tarefas que já foram concluídas, abra o menu de contexto do node secundário **Logs de tarefas** e selecione **Limpar**.
   - Caso deseje limpar o log de uma tarefa individual, no painel de resultados, abra o menu de contexto do log de tarefas que deseja limpar e selecione **Remover**.
   - Caso deseje limpar os logs de várias tarefas:
     a. No painel de resultados, utilize a tecla **Ctrl** ou **Shift** para selecionar os logs de tarefas que deseja limpar.
     b. Abra o menu de contexto de qualquer log de tarefas selecionado e selecione **Remover**.
4. Clique no botão **Sim** na janela de confirmação de exclusão para confirmar que deseja excluir os logs.

Os logs de tarefas selecionados serão limpos. A exclusão de logs de tarefas será registrada no log de auditoria do sistema.

Log de segurança

O Kaspersky Embedded Systems Security for Windows mantém um log de eventos associados a violações de segurança ou tentativas de violação no dispositivo 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).

É possível limpar o log de Segurança. Além disso, o Kaspersky Embedded Systems Security for Windows registra um evento de auditoria do sistema quando o Log de segurança é limpo.

Visualizando o log de eventos do Kaspersky Embedded Systems Security for Windows no Visualizador de eventos

É possível visualizar o log de eventos do Kaspersky Embedded Systems Security for Windows usando o snap-in Visualizador de Eventos do Microsoft Windows para o Console de Gerenciamento Microsoft. O log contém eventos registrados pelo Kaspersky Embedded Systems Security for Windows e necessários para diagnosticar falhas em sua operação.

Os eventos que serão registrados no log de eventos podem ser selecionados de acordo com os seguintes critérios:

- **por tipos de eventos**.
- **por nível de detalhamento**. O nível de detalhamento corresponde ao nível de importância dos eventos registrados no log (eventos informativos, importantes ou críticos). O mais detalhado é o nível Informativo, que registra todos os eventos. O menos detalhado é o nível Crítico, que registra apenas os eventos críticos.

Para visualizar o log de eventos do Kaspersky Embedded Systems Security for Windows:

1. Clique no botão **Iniciar**, insira o comando `mmc` na barra de pesquisa e pressione **ENTER**.

   O Console de Gerenciamento da Microsoft é aberto.

2. Selecione **Arquivo** > **Adicionar ou remover snap-in**.

   A janela **Adicionar ou remover snap-ins** é exibida.

3. Na lista de snap-ins disponíveis, selecione o snap-in **Visualizador de Eventos** e clique no botão **Adicionar**.

   A janela **Selecionar computador** é exibida.

4. Na janela **Selecionar computador**, especifique o dispositivo protegido no qual o Kaspersky Embedded Systems Security for Windows está instalado e clique em **OK**.

5. Na janela **Adicionar e remover snap-ins**, clique em **OK**.

   Na árvore do Console de Gerenciamento da Microsoft, o node **Visualizador de Eventos** aparece.

6. Expanda o node **Visualizador de Eventos** e selecione o node secundário **Logs de Aplicativos e Serviços** > **Kaspersky Embedded Systems Security for Windows**.

O log de evento do Kaspersky Embedded Systems Security for Windows é exibido.

Definindo as configurações de log por meio do Console do Aplicativo

É possível editar as seguintes configurações de logs do Kaspersky Embedded Systems Security for Windows:

- Duração do período de armazenamento para eventos em logs de tarefas e no log de auditoria do sistema.
- Localização da pasta onde o Kaspersky Embedded Systems Security for Windows armazena arquivos de log de tarefas e o arquivo do log de auditoria do sistema.

- Limites de geração de eventos para *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*.
- Eventos que o Kaspersky Embedded Systems Security for Windows salva em logs de tarefas, no log de auditoria do sistema e no log de eventos do Kaspersky Embedded Systems Security for Windows no Visualizador de eventos.
- Configurações para publicar eventos de auditoria e eventos de desempenho de tarefa para o servidor syslog através do protocolo Syslog.

Para definir as configurações de log usando o Console do Aplicativo:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Logs e notificações** e selecione **Propriedades**.

   A janela **Configurações de logs e notificações** é exibida.

2. Na guia **Geral**, caso necessário, selecione os eventos que o Kaspersky Embedded Systems Security for Windows salvará em logs de tarefas, no log de auditoria do sistema e no log de eventos do Kaspersky Embedded Systems Security for Windows no Visualizador de Eventos:

   a. Na lista **Componente**, selecione o componente do Kaspersky Embedded Systems Security for Windows para o qual deseja configurar o nível de detalhe.

   b. Na lista **Nível de importância**, selecione um nível de detalhe para eventos em logs de tarefas, no log de auditoria do sistema e no log de eventos para o componente selecionado.

      Na tabela seguinte com uma lista de eventos, as caixas de seleção são marcadas junto de eventos registrados em logs de tarefas, no log de auditoria do sistema e no log de eventos, de acordo com o nível de detalhe atual.

   c. Caso queira apagar manualmente o registro de eventos específicos para um componente selecionado ou tarefa:

      1. Na lista **Nível de importância**, selecione **Personalizado**.

      2. Na tabela com a lista de eventos, selecione as caixas de seleção junto dos eventos que você deseja que sejam registrados em logs de tarefas, no log de auditoria do sistema e no log de eventos.

3. Na guia **Avançado**, defina as configurações de armazenamento de logs e os limites de geração de evento para o status de proteção do dispositivo:

   - No bloco **Armazenamento de logs**:
     - **Pasta de logs**
     - **Remover logs de tarefas com mais de (dias)**
     - **Remover do sistema eventos de log de auditoria com mais de (dias)**
   - No bloco **Limites de geração de evento**, especifique quantos dias depois 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* ocorrerão.

4. Na guia **Integração SIEM**, defina as configurações para publicar eventos de auditoria e eventos de desempenho da tarefa no servidor syslog.

5. Clique no botão **OK** para salvar as alterações.

Sobre a integração SIEM

Para reduzir a carga nos dispositivos de baixo desempenho e reduzir o risco de degradação do sistema como resultado do aumento do tamanho de logs do aplicativo, é possível configurar a publicação de eventos de auditoria e de desempenho de tarefa no *servidor syslog* por meio do protocolo Syslog.

Um servidor syslog é um servidor externo para eventos de agregação (SIEM). Ele armazena e analisa os eventos recebidos e executa outras ações de gerenciamento de logs.

É possível usar a integração SIEM de duas maneiras:

- Eventos duplicados no servidor syslog: nesse modo, todos os eventos de desempenho de tarefa cuja publicação esteja definida nas configurações de logs, bem como todos os eventos de auditoria do sistema, continuam a ser armazenados no dispositivo protegido mesmo após terem sido enviados ao servidor SIEM.

  Recomenda-se usar este modo para reduzir o máximo possível a carga no dispositivo protegido.

- Excluir cópias locais de eventos: nesse modo, todos os eventos registrados durante a operação do aplicativo e publicados no servidor SIEM serão excluídos do dispositivo protegido.

  O aplicativo nunca exclui versões locais do log de segurança.

O Kaspersky Embedded Systems Security for Windows 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 servidor SIEM. O aplicativo é compatível com a conversão para um formato de dados estruturados e para o formato JSON.

Recomendamos selecionar o formato de eventos com base na configuração do servidor SIEM utilizado.

Configurações de confiabilidade

É possível reduzir o risco de retransmissão malsucedida de eventos ao servidor SIEM definindo 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.

O Kaspersky Embedded Systems Security for Windows também usa eventos de auditoria do sistema para notificar você sobre tentativas malsucedidas de conectar-se ao servidor SIEM e sobre erros ao enviar eventos ao servidor SIEM.

Definições das configurações de integração SIEM

Por padrão, a integração SIEM não é utilizada. É possível ativar e desativar a integração SIEM e definir configurações relevantes (consulte a tabela abaixo).

Configurações de integração SIEM

Configuração	Valor padrão	Descrição
Enviar eventos para um servidor syslog remoto pelo	Não aplicado	É possível ativar ou desativar a integração SIEM marcando ou desmarcando a caixa de seleção, respectivamente.

protocolo syslog		
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 terem sido enviados ao servidor 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 servidor SIEM.
Protocolo de conexão	TCP	É possível usar a lista suspensa para configurar a conexão com o servidor syslog principal e o refletido através dos protocolos UDP ou TCP.
Configurações de conexão do servidor syslog principal	Endereço IP: 127.0.0.1 Porto: 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.
Use um 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 Porto: 514	Você pode usar os campos apropriados para configurar o endereço IP e a porta usados para conectar-se ao servidor syslog de espelhamento. É possível especificar o endereço IP somente no formato IPv4.

Para definir as configurações de integração com o SIEM:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Logs e notificações**.
2. Selecione **Propriedades**.

   A janela **Configurações de logs e notificações** é exibida.
3. Selecione a guia **Integração SIEM**.
4. No bloco **Configurações de integração**, marque a caixa de seleção **Enviar eventos para um servidor syslog remoto pelo protocolo syslog**.
5. Caso necessário, no bloco **Configurações de integração**, marque a caixa de seleção **Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto**.

   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.
6. No bloco **Formato dos eventos**, especifique o formato para o qual deseja converter eventos do aplicativo para que sejam enviados ao servidor SIEM.

   Por padrão, o aplicativo converte-os em um formato de dados estruturados.
7. No bloco **Configurações de conexão**:

- Especifique o protocolo de conexão SIEM.
- Nos campos de mesmo nome, especifique o endereço IPv4 e a porta para a conexão com o servidor syslog principal.
- Marque a caixa de seleção **Use um 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.
- Nos campos de mesmo nome, especifique o endereço IPv4 e a porta para a conexão com um servidor syslog adicional.

8. Clique no botão **OK**.

   As configurações da integração SIEM definidas serão aplicadas.

Definindo as configurações de logs e notificações por meio do Plugin de Administração

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 for Windows e ao status de proteção de antivírus no dispositivo:

- O administrador pode receber informações sobre eventos de tipos selecionados.
- Os usuários de LAN que acessam o dispositivo protegido e os usuários do dispositivo de terminal protegido podem receber informações sobre eventos de *Objeto detectado*.

As notificações sobre os eventos do Kaspersky Embedded Systems Security for Windows podem ser configuradas para um único dispositivo protegido usando a janela **Propriedades: <Nome do dispositivo protegido>** do dispositivo protegido selecionado ou para um grupo de dispositivos protegidos na janela **Propriedades: <Nome da política>** do grupo de administração selecionado.

Na guia **Notificações de evento** 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 **Notificações de evento** (a guia padrão no 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**.

É possível configurar notificações para alguns tipos de eventos somente na janela ou na guia; é possível 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 **Notificações de evento** e na janela **Configurações de notificação**, o administrador do sistema receberá notificações desses eventos duas vezes, mas no mesmo modo.

Definindo as configurações de logs de tarefa

Para configurar os logs do Kaspersky Embedded Systems Security for Windows, execute as seguintes etapas:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do log para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para configurar o aplicativo para um único dispositivo protegido individual, selecione a guia **Dispositivos** e vá para as configurações do aplicativo.
4. Na seção **Logs e notificações**, clique no botão **Configurações** no bloco **Logs de tarefas**.
5. A janela **Configurações de registros** é exibida na guia **Logs**.
6. Configure o nível de detalhe de eventos em logs:
   a. Na lista **Componente**, selecione o componente do Kaspersky Embedded Systems Security for Windows para o qual deseja configurar o nível de detalhe.
   b. Na lista **Nível de importância**, selecione um nível de detalhe para eventos em logs de tarefas, no log de auditoria do sistema e no log de eventos para o componente selecionado.
      Na tabela seguinte com uma lista de eventos, as caixas de seleção são marcadas junto de eventos registrados em logs de tarefas, no log de auditoria do sistema e no log de eventos, de acordo com o nível de detalhe atual.
   c. Caso queira apagar manualmente o registro de eventos específicos para um componente selecionado ou tarefa:
      1. Na lista **Nível de importância**, selecione **Personalizado**.
      2. Na tabela com a lista de eventos, selecione as caixas de seleção junto dos eventos que você deseja que sejam registrados em logs de tarefas, no log de auditoria do sistema e no log de eventos.
7. No bloco **Armazenamento de logs**, defina as configurações de armazenamento de log:
   - **Pasta de logs**
   - **Remover logs de tarefas com mais de (dias)**
   - **Remover do sistema eventos de log de auditoria com mais de (dias)**
8. Na guia **Integração SIEM**, defina as configurações para publicar eventos de auditoria e eventos de desempenho da tarefa no servidor syslog.
9. Clique no botão **OK**.

As configurações de log definidas são salvas.

Log de segurança

O Kaspersky Embedded Systems Security for Windows mantém um log de eventos associados a violações de segurança ou tentativas de violação no dispositivo 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).

É possível limpar o log de Segurança. Além disso, o Kaspersky Embedded Systems Security for Windows registra um evento de auditoria do sistema quando o Log de segurança é limpo.

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 do aumento do tamanho de logs do aplicativo, é possível configurar a publicação de eventos de auditoria e de desempenho de tarefa no *servidor syslog* por meio do protocolo Syslog.

Um servidor syslog é um servidor externo para eventos de agregação (SIEM). Ele armazena e analisa os eventos recebidos e executa outras ações de gerenciamento de logs.

É possível usar a integração SIEM de duas maneiras:

- Eventos duplicados no servidor syslog: nesse modo, todos os eventos de desempenho de tarefa cuja publicação esteja definida nas configurações de logs, bem como todos os eventos de auditoria do sistema, continuam a ser armazenados no dispositivo protegido mesmo após terem sido enviados ao servidor SIEM.

  Recomenda-se usar este modo para reduzir o máximo possível a carga no dispositivo protegido.

- Excluir cópias locais de eventos: nesse modo, todos os eventos registrados durante a operação do aplicativo e publicados no servidor SIEM serão excluídos do dispositivo protegido.

  O aplicativo nunca exclui versões locais do log de segurança.

O Kaspersky Embedded Systems Security for Windows 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 servidor SIEM. O aplicativo é compatível com a conversão para um formato de dados estruturados e para o formato JSON.

É possível reduzir o risco de retransmissão malsucedida de eventos ao servidor SIEM definindo 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 configurações relevantes (consulte a tabela abaixo).

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 terem sido enviados ao servidor 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 servidor SIEM.
Protocolo de conexão	TCP	É possível usar a lista suspensa para configurar a conexão com o servidor syslog principal via protocolos UDP ou TCP; e com o servidor syslog de espelhamento pelo protocolo TCP.
Configurações de conexão do servidor syslog principal	Endereço IP: 127.0.0.1 Porto: 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.
Use um 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 Porto: 514	Você pode usar os campos apropriados para configurar o endereço IP e a porta usados para conectar-se ao servidor syslog de espelhamento. É possível especificar o endereço IP somente no formato IPv4.

Para definir as configurações de integração com o SIEM:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do log para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

   - Para configurar o aplicativo para um único dispositivo protegido individual, selecione a guia **Dispositivos** e vá para as configurações do aplicativo.

4. Na seção **Logs e notificações**, clique no botão **Logs de tarefas** no bloco **Configurações**.

   A janela **Configurações de logs e notificações** é exibida.

5. Selecione a guia **Integração SIEM**.

6. No bloco **Configurações de integração**, marque a caixa de seleção **Enviar eventos para um servidor syslog remoto pelo protocolo syslog**.

7. Caso necessário, no bloco **Configurações de integração**, marque a caixa de seleção **Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto**.

   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.

8. No bloco **Formato dos eventos**, especifique o formato para o qual deseja converter eventos do aplicativo para que sejam enviados ao servidor SIEM.

   Por padrão, o aplicativo converte-os em um formato de dados estruturados.

9. No bloco **Configurações de conexão**:

   - Especifique o protocolo de conexão SIEM.
   - Nos campos de mesmo nome, especifique o endereço IPv4 e a porta para a conexão com o servidor syslog principal.
   - Marque a caixa de seleção **Use um 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.
   - Nos campos de mesmo nome, especifique o endereço IPv4 e a porta para a conexão com um servidor syslog adicional.

10. Clique no botão **OK**.

As configurações da integração SIEM definidas serão aplicadas.

Definição de configurações de notificação

Para configurar as notificações do Kaspersky Embedded Systems Security for Windows:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Logs e notificações**, clique no botão **Notificações de evento** na subseção **Configurações**.

5. Na janela **Configurações de notificação**, defina as seguintes configurações do Kaspersky Embedded Systems Security for Windows de acordo com seus requisitos:

   - Na lista **Configurações de notificação**, selecione o tipo de notificação cujas configurações deseja definir.
   - Na seção **Notificar usuários**, configure o método de notificação do usuário. Se necessário, insira o texto da mensagem de notificação.
   - Na seção **Notificar administradores**, configure o método de notificação do 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 quanto tempo depois o Kaspersky Embedded Systems Security for Windows deverá registrar 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 banco dados do aplicativo está muito desatualizado (dias)**
     - **A Verificação de áreas críticas não é executada há muito tempo (dias)**

6. Clique no botão **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 for Windows envia informações ao Servidor de Administração do Kaspersky Security Center:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Logs e notificações**, clique no botão **Interação com o Servidor de Administração** na subseção **Configurações**.

   A janela **Listas da rede do Servidor de Administração** é exibida.

5. Na janela **Listas da rede do Servidor de Administração**, escolha os tipos de objetos sobre os quais o Kaspersky Embedded Systems Security for Windows enviará informações ao Servidor de Administração do Kaspersky Security Center:

   - Objetos em Quarentena.

- Objetos do Backup.

6. Clique no botão **OK**.

   O Kaspersky Embedded Systems Security for Windows enviará informações sobre os tipos de objetos selecionados para o Servidor de Administração.

Configurações de notificação

Esta seção fornece informações sobre as formas em que os usuários e administradores do Kaspersky Embedded Systems Security for Windows podem ser notificados sobre eventos do aplicativo e o status de proteção do dispositivo, bem como instruções sobre como configurar notificações.

Métodos de notificação do administrador e dos usuários

É possível configurar o aplicativo para notificar o administrador e usuários que acessem o dispositivo sobre os seguintes eventos na operação do Kaspersky Embedded Systems Security for Windows e o status da proteção antivírus no dispositivo.

- O administrador pode receber informações sobre eventos de tipos selecionados.
- Os usuários de LAN que acessam um dispositivo e os usuários do dispositivo de terminal podem receber informações sobre eventos do tipo *Objeto detectado* na tarefa de Proteção de Arquivos em Tempo Real.

No Console do Aplicativo, as notificações de administrador ou usuário podem ser ativadas usando vários métodos:

- Métodos de notificação do usuário:
  a. Ferramentas do serviço de terminal.
     É possível aplicar esse método para notificar usuários do dispositivo de terminal protegido se o dispositivo protegido for usado como terminal.
  b. Ferramentas do serviço de mensagem.
     Você pode aplicar esse método para notificação através de serviços de mensagens do Microsoft Windows.
- Métodos de notificação do administrador:
  a. Ferramentas do serviço de mensagem.
     Você pode aplicar esse método para notificação através de serviços de mensagens do Microsoft Windows.
  b. Executando um arquivo executável.
     Esse método executa um arquivo executável armazenado na unidade local do dispositivo protegido quando um evento ocorre.
  c. Enviar por e-mail.
     Esse método usa e-mail para transmitir mensagens.

É possível criar o texto de uma mensagem para tipos de eventos individuais. Elas podem incluir um campo de informações para descrever um evento. Por padrão, o aplicativo usa uma mensagem padrão para notificar os usuários.

Configurando notificações do administrador e dos usuários

As configurações de notificação de eventos oferecem opções de métodos para configurar e compor uma mensagem.

Para definir as configurações de notificação de eventos:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Logs e notificações** e selecione **Propriedades**.

   A janela **Configurações de logs e notificações** é exibida.

2. Na guia **Notificações**, selecione o modo de notificação:

   a. Selecione o evento para o qual você deseja selecionar um método de notificação na lista **Tipo de evento**.

   b. Nas configurações de grupo **Notificar administradores** ou **Notificar usuários**, selecione a caixa de seleção junto aos métodos de notificação que deseja configurar.

   > Só é possível configurar as notificações de usuário para os eventos: **Objeto detectado**, **Dispositivo externo não confiável detectado e restrito** e **Sessão de rede listada como não confiável**.

3. Para adicionar o texto de uma mensagem:

   a. Clique no botão **Texto da mensagem**.

   b. Na janela que se abre, insira o texto a ser exibido no evento de mensagem correspondente.

   > É possível criar a mesma mensagem para vários tipos de eventos: após selecionar um método de notificação para um tipo de evento, use a tecla **Ctrl** ou **Shift** para selecionar os outros tipos de eventos para os quais deseja usar a mesma mensagem e, em seguida, clique no botão **Texto da mensagem**.

   a. Para adicionar campos com informações sobre um evento, clique no botão **Macro** e selecione os campos relevantes na lista suspensa. Os campos com informações do evento estão descritos na tabela nesta seção.

   b. Para restaurar o texto padrão da mensagem de evento, clique no botão **Por padrão**.

4. Para configurar como os administradores serão notificados sobre um evento selecionado, selecione a guia **Notificações** e, na seção **Configurações**, clique no botão **Notificar administradores**. Em seguida, na janela **Configurações avançadas**, configure os métodos de notificação selecionados. Para isso, execute as seguintes ações:

   a. Para notificações por e-mail, abra a guia **E-mail** e especifique os endereços de e-mail de destinatários (separe os endereços com ponto e vírgula), nome ou endereço de rede do servidor SMTP e número da porta nos campos adequados. Se necessário, especifique o texto que será exibido nos campos **Assunto** e **De**. O texto no campo **Assunto** também pode incluir variáveis com informações sobre o evento (consulte a tabela abaixo).

   Se deseja aplicar a autenticação da conta ao se conectar ao servidor SMTP, selecione **Configurações de autenticação** no grupo **Usar autenticação SMTP** e especifique o nome e a senha do usuário cuja conta de usuário será autenticada.

   b. Para notificações usando o serviço Windows Messenger, crie uma lista de dispositivos protegidos destinatários de notificações na guia **Windows Messenger Service**: para cada dispositivo protegido que deseja adicionar, clique no botão **Adicionar** e insira seu nome de rede no campo de entrada.

   c. Para executar um arquivo executável, na guia **Arquivo executável**, selecione um arquivo na unidade local do dispositivo protegido ou insira o caminho completo para ele. Esse arquivo será executado no dispositivo protegido quando o evento ocorrer. Insira o nome de usuário e a senha que serão usados para executar o arquivo.

   As variáveis de ambiente do sistema podem ser usadas ao especificar o caminho do arquivo executável; não são permitidas variáveis de ambiente do usuário.

Caso deseje limitar o número de mensagens de um tipo de evento ao longo de um período de tempo, na guia **Avançado** selecione **Não enviar a mesma notificação mais de** e especifique o número de vezes e um intervalo de tempo.

5. Clique no botão **OK**.

As configurações de notificação definidas são salvas.

Campos com informações de eventos

Variável	Descrição
%EVENT_TYPE%	Tipo de evento.
%EVENT_TIME%	Hora do evento.
%EVENT_SEVERITY%	Nível de importância.
%OBJECT%	Nome do objeto (nas tarefas de Proteção do Computador em Tempo Real e de Verificação por Demanda). A tarefa de Atualização dos Módulos de Software inclui o nome da atualização e o endereço da página da Web com as informações sobre a atualização.
%VIRUS_NAME%	O nome do objeto de acordo com a classificação da Virus Encyclopedia. Esse nome é incluído no nome completo de um objeto detectado que o Kaspersky Embedded Systems Security for Windows devolve ao detectar um objeto. É possível exibir o nome completo de um objeto detectado no log de tarefas.
%VIRUS_TYPE%	O tipo de objeto detectado de acordo com a classificação da Kaspersky, como "vírus" ou "Cavalo de troia". É incluído no nome completo de um objeto detectado, que é devolvido pelo Kaspersky Embedded Systems Security for Windows quando ele identifica um objeto infectado ou possivelmente infectado. Você pode exibir o nome completo de um objeto detectado no Log de tarefas.
%USER_COMPUTER%	Nas tarefas Proteção de Arquivos em Tempo Real, o nome do dispositivo protegido do usuário que acessou o objeto no dispositivo.
%USER_NAME%	Nas tarefas Proteção de Arquivos em Tempo Real, o nome do usuário que acessou o objeto no dispositivo.
%FROM_COMPUTER%	Nome do dispositivo protegido no qual a notificação foi gerada.
%EVENT_REASON%	Motivo do evento (alguns eventos não contêm esse campo).
%ERROR_CODE%	Código do erro (apenas para o evento "erro de tarefa interno").
%TASK_NAME%	Nome da tarefa (somente para eventos relacionados ao desempenho de tarefas).

Inicialização e interrupção do Kaspersky Embedded Systems Security for Windows

Esta seção contém informações sobre como iniciar o Console do Aplicativo e como iniciar e interromper o Kaspersky Security Service.

Inicialização do Plug-in de Administração do Kaspersky Embedded Systems Security for Windows

Nenhuma ação adicional é necessária para iniciar o Plug-in de Administração do Kaspersky Embedded Systems Security for Windows no Kaspersky Security Center. Quando o Plug-in de Administração for instalado no dispositivo protegido do administrador, ele será iniciado juntamente com o Kaspersky Security Center. Informações detalhadas sobre a inicialização do Kaspersky Security Center podem ser encontradas na *Ajuda do Kaspersky Security Center*.

Inicialização do Console do Kaspersky Embedded Systems Security for Windows no menu Iniciar

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

*Para iniciar o Console do Aplicativo no menu **Iniciar**:*

1. No menu **Iniciar**, selecione **Programas** > **Kaspersky Embedded Systems Security for Windows** > **Ferramentas de Administração** > **Console do Kaspersky Embedded Systems Security for Windows**.

Para adicionar outros snap-ins ao Console do Aplicativo, inicie o Console do Aplicativo no modo de autor.

Para iniciar o Console do Aplicativo no modo de autor:

1. No menu **Iniciar**, selecione **Programas** > **Kaspersky Embedded Systems Security for Windows** > **Ferramentas de Administração**.
2. No menu de contexto do Console do Aplicativo, selecione o comando **Autor**.

O Console do Aplicativo é iniciado no modo de autor.

Se o Console do Aplicativo for iniciado no dispositivo protegido, a janela do Console do Aplicativo é exibida.

Caso tenha iniciado o Console do Aplicativo em um dispositivo não protegido, conecte-se ao dispositivo protegido.

Para conectar-se ao dispositivo protegido:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Kaspersky Embedded Systems Security for Windows**.
2. Selecione o comando **Conectar a outro computador**.

   A janela **Selecionar dispositivo protegido** é exibida.

3. Selecione **Outro dispositivo** na janela exibida.

4. Especifique o nome da rede do dispositivo protegido no campo de entrada à direita.

5. Clique no botão **OK**.

O Console do Aplicativo será conectado ao dispositivo protegido.

Se a conta de usuário que você está usando para iniciar a sessão no Microsoft Windows não tiver permissões suficientes para acessar o Kaspersky Security Management Service no dispositivo protegido, marque a caixa de seleção **Conectar como usuário** e especifique uma conta de usuário com as permissões necessárias.

Inicialização e interrupção do Kaspersky Security Service

Por padrão, o Kaspersky Security Service é iniciado automaticamente imediatamente após a inicialização do sistema operacional. O Kaspersky Security Service gerencia os processos de trabalho que executam as tarefas de Proteção do Computador em Tempo Real, Controle do Computador, Verificação por Demanda e Atualização.

Por padrão, quando o Kaspersky Embedded Systems Security for Windows 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 serem iniciadas **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 programadas para serem executadas **Ao iniciar o aplicativo**. Outras tarefas devem ser iniciadas manualmente.

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

Você pode iniciar e interromper o Kaspersky Embedded Systems Security for Windows se for membro do grupo de Administradores no dispositivo protegido.

Para interromper ou iniciar o aplicativo usando o Console do Aplicativo:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Kaspersky Embedded Systems Security for Windows**.

2. Selecione um dos seguintes itens:

   - **Parar o serviço**
   - **Iniciar o serviço**

O Kaspersky Security Service será iniciado ou interrompido.

Inicialização dos componentes do Kaspersky Embedded Systems Security for Windows no modo seguro do sistema operacional

Esta seção fornece informações sobre o funcionamento do Kaspersky Embedded Systems Security for Windows no modo seguro do sistema operacional.

Sobre o funcionamento do Kaspersky Embedded Systems Security for Windows no modo seguro do sistema operacional

Os componentes do Kaspersky Embedded Systems Security for Windows podem ser inicializados quando o sistema operacional é inicializado no modo seguro. Além do Kaspersky Security Service (kavfs.exe), o driver klam.sys é carregado. Ele é usado para registrar o Kaspersky Security Service como um serviço protegido durante o início do sistema operacional. Para obter mais detalhes, consulte a seção Registrar o Kaspersky Security Service como um serviço protegido.

O Kaspersky Embedded Systems Security for Windows pode ser iniciado nos seguintes modos seguros do sistema operacional:

- Modo seguro mínimo – Esse modo é inicializado quando a opção padrão do modo seguro do sistema operacional é selecionada. Nesse caso, o Kaspersky Embedded Systems Security for Windows pode iniciar os seguintes componentes:
  - Proteção de Arquivos em Tempo Real.
  - Verificação por Demanda.
  - Controle de Inicialização de Aplicativos e Gerador de Regras de Controle de Inicialização de Aplicativos.
  - Inspeção do Log.
  - Monitor de Integridade de Arquivos.
  - Monitor de Comparação de Integridade de Arquivos.
  - Controle de Integridade de Aplicativos.

Modo seguro com rede – Nesse modo, o sistema operacional é inicializado no modo seguro com drivers de rede. Além dos componentes iniciados no Modo Seguro Mínimo, o Kaspersky Embedded Systems Security for Windows pode iniciar os seguintes componentes nesse modo:

- Atualização do Banco de Dados.
- Atualização dos Módulos de Software.

Inicialização do Kaspersky Embedded Systems Security for Windows no modo seguro

Por padrão, o Kaspersky Embedded Systems Security for Windows não é iniciado quando o sistema operacional é inicializado no modo seguro.

Para fazer com que o Kaspersky Embedded Systems Security for Windows seja inicializado no modo seguro do sistema operacional:

1. Inicie o Editor de registro do Windows (C:\Windows\regedit.exe).

2. Abra a chave [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] do registro de sistema.

3. Abra o parâmetro LoadInSafeMode.

4. Defina o valor para `1`.

5. Clique no botão **OK**.

Para cancelar a inicialização do Kaspersky Embedded Systems Security for Windows no modo seguro do sistema operacional:

1. Inicie o Editor de registro do Windows (C:\Windows\regedit.exe).

2. Abra a chave [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] do registro de sistema.

3. Abra o parâmetro LoadInSafeMode.

4. Defina o valor para `0`.

5. Clique no botão **OK**.

Autodefesa do Kaspersky Embedded Systems Security for Windows

Esta seção fornece informações sobre os mecanismos de autodefesa do Kaspersky Embedded Systems Security for Windows.

Sobre a autodefesa do Kaspersky Embedded Systems Security for Windows

O Kaspersky Embedded Systems Security for Windows tem mecanismos de autodefesa que protegem o aplicativo contra modificação ou exclusão de suas pastas, processos de memória e entradas de registro de sistema.

Proteção contra alterações em pastas com componentes do Kaspersky Embedded Systems Security for Windows instalados

O Kaspersky Embedded Systems Security for Windows bloqueia a renomeação e exclusão de pastas com os componentes do aplicativo instalado por qualquer conta de usuário. Por padrão, os caminhos das pastas de instalação do aplicativo são os seguintes:

- Para a 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 Lab\Kaspersky Embedded Systems Security\

Proteção contra alterações em chaves de registro do Kaspersky Embedded Systems Security for Windows

O Kaspersky Embedded Systems Security for Windows restringe o acesso às seguintes chaves e bifurcações de registro, que facilitam o carregamento dos drivers e serviços do aplicativo:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3] (no Microsoft Windows de 64 bits)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\Trace]

Os direitos de alterar essas chaves e bifurcações de registro são concedidos apenas à conta Sistema Local (SYSTEM). As contas de usuário e Administrador recebem direitos de somente leitura.

Proteção contra alterações na memória das partes de serviço do programa

Para proteger as partes de serviço do programa de processos de terceiros, os drivers do Kaspersky Embedded Systems Security for Windows restringem o acesso aos seguintes arquivos executáveis:

- kavfs.exe
- kavfswp.exe
- kavfswh.exe
- kavfsgt.exe

Por padrão, o acesso à memória das partes de serviço do Kaspersky Embedded Systems Security for Windows é restrito para processos de terceiros.

É possível ativar as funções de autodefesa nas propriedades de política do Console do Kaspersky Embedded Systems Security for Windows e do Plug-in de Administração do Kaspersky Embedded Systems Security for Windows.

Registrar o Kaspersky Security Service como um serviço protegido

A tecnologia *Processo protegido superficial* ("PPL") garante que o sistema operacional carregará apenas os serviços e processos confiáveis. Para iniciar um serviço como serviço protegido, um driver *Early Launch Antimalware* deve ser instalado no dispositivo protegido.

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

Um driver ELAM é instalado automaticamente durante a instalação do Kaspersky Embedded Systems Security for Windows e é usado para registrar o Kaspersky Security Service como um PPL quando o sistema operacional for inicializado. Quando o Kaspersky Security Service (KAVFS) 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, independentemente das permissões de usuário atribuídas. O registro do Kaspersky Security Service como PPL usando o driver ELAM é compatível com o Microsoft Windows 10 e sistemas operacionais posteriores. Caso o Kaspersky Embedded Systems Security for Windows seja instalado em um servidor que executa um sistema operacional compatível com PPL, o gerenciamento de permissões não estará disponível para o Kaspersky Security Service (KAVFS).

Para instalar o Kaspersky Embedded Systems Security for Windows como um PPL, execute o seguinte comando:

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security for Windows

Esta seção contém informações sobre permissões para gerenciar o Kaspersky Embedded Systems Security for Windows e serviços de sistemas operacionais registrados pelo aplicativo, bem como as instruções sobre como configurar essas permissões.

Sobre permissões para gerenciar o Kaspersky Embedded Systems Security for Windows

Por padrão, o acesso a todas as funções do Kaspersky Embedded Systems Security for Windows é concedido aos usuários do grupo "Administradores" no dispositivo protegido, aos usuários do grupo Administradores de ESS criado no dispositivo protegido durante a instalação do Kaspersky Embedded Systems Security for Windows e ao grupo SYSTEM.

Usuários com nível de acesso de Permissões de edição do Kaspersky Embedded Systems Security for Windows podem conceder acesso às funções do Kaspersky Embedded Systems Security for Windows a outros usuários registrados no dispositivo protegido ou incluídos no domínio.

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

Você pode escolher um dos seguintes níveis predefinidos de acesso 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 for Windows, configurações de componentes e permissões de usuários do Kaspersky Embedded Systems Security for Windows; além da capacidade de visualizar estatísticas do Kaspersky Embedded Systems Security for Windows.

- **Modificação** – acesso a todas as funções do aplicativo, exceto à edição das permissões de usuário: capacidade de visualizar e editar as configurações gerais do Kaspersky Embedded Systems Security for Windows e as configurações de componentes do Kaspersky Embedded Systems Security for Windows.

- **Ler** – capacidade de visualizar as configurações gerais do Kaspersky Embedded Systems Security for Windows, configurações de componentes do Kaspersky Embedded Systems Security for Windows, estatísticas do Kaspersky Embedded Systems Security for Windows e permissões de usuário do Kaspersky Embedded Systems Security for Windows.

Também é possível configurar permissões de acesso avançadas: permitir ou bloquear acesso a funções específicas do Kaspersky Embedded Systems Security for Windows.

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.

Sobre permissões de acesso para funções do Kaspersky Embedded Systems Security for Windows

Direitos de usuário	Descrição
Gerenciamento de tarefas	Capacidade para iniciar/parar/pausar/reiniciar tarefas do Kaspersky Embedded Systems Security for Windows.
Criar e excluir tarefas de	Capacidade para criar e excluir tarefas de Verificação por Demanda.

Verificação por Demanda	
Editar configurações	Capacidade para: • Importar as configurações do Kaspersky Embedded Systems Security for Windows a partir de um arquivo de configuração. • Editar as configurações do aplicativo.
Configurações de leitura	Capacidade para: • Visualizar as configurações gerais e configurações de tarefas do Kaspersky Embedded Systems Security for Windows. • Exportar as configurações do Kaspersky Embedded Systems Security for Windows para um arquivo de configuração. • Visualizar 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 de visualizar estatísticas de cada tarefa do Kaspersky Embedded Systems Security for Windows.
Licenciamento do aplicativo	Capacidade de ativar o Kaspersky Embedded Systems Security for Windows.
Desinstalar o aplicativo	Capacidade de desinstalar o Kaspersky Embedded Systems Security for Windows.
Permissões de leitura	Capacidade de visualizar a lista de usuários do Kaspersky Embedded Systems Security for Windows e privilégios de acesso dos usuários.
Permissões de edição	Capacidade para: • Editar a lista de usuários com acesso ao gerenciamento de aplicativos. • Editar permissões de acesso de usuário às funções do Kaspersky Embedded Systems Security for Windows.

Sobre permissões de gerenciamento de serviços registrados

Durante a instalação, o Kaspersky Embedded Systems Security for Windows registra no Windows o Kaspersky Security Service (KAVFS), o Kaspersky Security Management Service (KAVFSGT) e o Serviço de Kaspersky Security Exploit Prevention (KAVFSSLP).

O Kaspersky Security Service pode ser registrado como um processo protegido Superficial usando o driver ELAM no Microsoft Windows 10 e sistemas operacionais posteriores. Quando um processo é iniciado como um PPL, ele não pode ser gerenciado pelo usuário, independentemente das permissões de usuário atribuídas. Se o Kaspersky Embedded Systems Security for Windows for instalado em um dispositivo protegido executando um sistema operacional compatível com PPL, o gerenciamento de permissões não estará disponível para o Kaspersky Security Service (KAVFS).

Kaspersky Security Service

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

Os usuários com Acesso de nível de permissões de edição podem conceder permissões de acesso para gerenciar o Kaspersky Security Service a outros usuários registrados no dispositivo protegido ou incluídos no domínio.

Kaspersky Security Management Service

Para gerenciar o aplicativo por meio do Console do Aplicativo instalado em um dispositivo protegido diferente, a conta cujas permissões foram usadas para conectar ao Kaspersky Embedded Systems Security for Windows deve ter acesso total ao Kaspersky Security Management Service no dispositivo protegido.

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

Só é possível gerenciar o Kaspersky Security Management Service por meio do snap-in Serviços do Microsoft Windows.

Serviço de Kaspersky Security Exploit Prevention

Por padrão, as permissões de acesso para gerenciar o Serviço de Kaspersky Security Exploit Prevention são concedidas aos usuários no grupo de Administradores no dispositivo protegido, assim como ao grupo SYSTEM com permissões de leitura e execução.

Sobre permissões de acesso para o Kaspersky Security Management Service

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

Durante a instalação, o Kaspersky Embedded Systems Security for Windows registra o Kaspersky Security Management Service (KAVFSGT). Para gerenciar o aplicativo por meio do Console do Aplicativo instalado em um dispositivo protegido diferente, a conta usada para conectar ao Kaspersky Embedded Systems Security for Windows deve ter acesso total ao Kaspersky Security Management Service no dispositivo protegido.

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

Só é possível gerenciar o Kaspersky Security Management Service 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 for Windows.

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

Sobre permissões para gerenciar o Kaspersky Security Service

Durante a instalação, o Kaspersky Embedded Systems Security for Windows 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 dispositivo protegido via Kaspersky Security Service, é possível restringir as permissões de gerenciamento para o Kaspersky Security Service no Console do Aplicativo ou no 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 dispositivo protegido. Permissões de leitura são concedidas aos grupos SERVICE e INTERACTIVE e permissões de leitura e execução são concedidas ao grupo SYSTEM.

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

Os usuários com acesso às funções do nível de Permissões de edição podem conceder permissões de acesso para gerenciar o Kaspersky Security Service a outros usuários registrados no dispositivo protegido ou incluídos no domínio.

É possível selecionar um dos seguintes níveis predefinidos de permissões de acesso para um usuário ou grupo de usuários do Kaspersky Embedded Systems Security for Windows 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 de 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 as permissões de acesso avançadas: permitir ou negar acesso a funções específicas do Kaspersky Embedded Systems Security for Windows (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.

Permissões de acesso para as funções do Kaspersky Security Service

Recurso	Descrição
Visualizar configurações de serviço	Capacidade de visualizar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
Solicitar status de serviço do Gerenciador de Controle de Serviço	Capacidade de solicitar o status de execução do Kaspersky Security Service pelo Gerenciador de Controle de Serviço do Microsoft Windows.
Solicitação de status de serviço	Capacidade de solicitar o status de execução do Kaspersky Security Service.
Ler lista de 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 interromper 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 usuários 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.

Gerenciamento de permissões de acesso por meio do Plug-in de Administração

Nesta seção, saiba como navegar pela interface do Plug-in de Administração e definir permissões de acesso para um ou todos os dispositivos protegidos na rede.

Configurando permissões de acesso para o Kaspersky Embedded Systems Security for Windows e o Kaspersky Security Service

É possível editar a lista de usuários e grupos de usuário com permissão para acessar as funções do Kaspersky Embedded Systems Security for Windows e gerenciar o Kaspersky Security Service. Também é possível editar as permissões de acesso desses usuários e grupos de usuário.

Para adicionar ou remover um usuário ou grupo da lista:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Suplementar**, execute uma das seguintes etapas:

   - Clique no botão **Configurações** na subseção **Permissões de acesso do usuário para gerenciamento do aplicativo** caso queira editar a lista de usuários com permissões de acesso para gerenciar as funções do Kaspersky Embedded Systems Security for Windows.

   - Clique no botão **Configurações** na subseção **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service** caso queira editar a lista de usuários com permissões de acesso para gerenciar o Kaspersky Security Service.

     A janela **Permissões para** o **Kaspersky Embedded Systems Security 3.3 for Windows** é exibida.

5. 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 ao qual 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**.

6. 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 for Windows ou o Kaspersky Security Service:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Suplementar**, execute uma das seguintes etapas:

   - Clique no botão **Configurações** na subseção **Permissões de acesso do usuário para gerenciamento do aplicativo** caso queira editar a lista de usuários com permissões de acesso para gerenciar as funções do

Kaspersky Embedded Systems Security for Windows.

- Clique no botão **Configurações** na subseção **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service** caso queira editar a lista de usuários com permissões de acesso para gerenciar o aplicativo pelo Kaspersky Security Service.

  A janela **Permissões para** o **Kaspersky Embedded Systems Security for Windows** é exibida.

5. Na janela exibida, na lista **Grupo ou nomes de usuário**, selecione o usuário ou grupo de usuários de quem você deseja alterar as permissões.

6. Na seção **Permissões para <Usuário (Grupo)>**, selecione as caixas de seleção **Permitir** ou **Negar** para os seguintes níveis de acesso:

   - **Controle total**: conjunto completo de permissões para gerenciar o Kaspersky Embedded Systems Security for Windows ou o Kaspersky Security Service.

   - **Ler**:

     - As seguintes permissões para gerenciar o Kaspersky Embedded Systems Security for Windows: **Recuperar estatísticas**, **Ler configurações**, **Ler registros** e **Permissões de leitura**.

     - As seguintes permissões para gerenciar o Kaspersky Security Service: **Ler as configurações de serviço**, **Solicitar status 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 for Windows, exceto **Permissões de edição**.

     - As seguintes permissões para gerenciar o Kaspersky Security Service: **Modificar configurações do serviço**, **Permissões de leitura**.

   - **Permissões especiais**: as seguintes permissões para gerenciar o Kaspersky Security Service: **Inicialização do serviço**, **Parar serviço**, **Pausar/retomar serviço**, **Permissões de leitura**, **Solicitações de serviço definidos pelo usuário**.

7. Para configurar permissões avançadas para um usuário ou grupo (**Permissões especiais**), clique no botão **Avançado**.

   a. Na janela exibida **Configurações avançadas de segurança para** o **Kaspersky Embedded Systems Security for Windows**, selecione o usuário ou grupo desejado.

   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 ao lado das funções que deseja permitir ou bloquear para o usuário ou grupo selecionado.

   e. Clique no botão **OK**.

   f. Na janela **Configurações de segurança avançadas para** o **Kaspersky Embedded Systems Security for Windows**, clique em **OK**.

8. Na janela **Permissões para** o **Kaspersky Embedded Systems Security for Windows**, clique no botão **Aplicar**.

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

Acesso protegido por senha às funções do Kaspersky Embedded Systems Security for Windows

Você pode restringir o acesso ao gerenciamento do aplicativo e aos serviços registrados configurando permissões de usuário. Também é possível estabelecer uma proteção por senha nas configurações do Kaspersky Embedded Systems Security for Windows para proteção adicional de operações críticas.

O Kaspersky Embedded Systems Security for Windows solicita uma senha quando você tenta acessar as seguintes funções do aplicativo:

- conectar-se ao Console do Aplicativo;
- desinstalar o Kaspersky Embedded Systems Security for Windows;
- modificar componentes do Kaspersky Embedded Systems Security for Windows;
- executar comandos da linha de comando.

A interface do Kaspersky Embedded Systems Security for Windows disfarça a senha especificada na tela. O Kaspersky Embedded Systems Security for Windows armazena a senha como uma soma de verificação calculada quando a senha é digitada.

O Kaspersky Embedded Systems Security for Windows não verifica o nível de segurança da senha e não bloqueia a entrada de senha após várias tentativas com falha.

Ao criar uma senha, é recomendado atender às seguintes condições:

- A senha não conter o nome da conta ou o nome do computador.
- A senha ter pelo menos oito caracteres.
- A senha conter caracteres que correspondam a pelo menos três das seguintes categorias:
  - letras latinas maiúsculas (A-Z);
  - letras latinas minúsculas (a-z);
  - números (0-9);
  - símbolos de ponto de exclamação (!), cifrão ($), sinal de cardinal (#) e sinal de porcentagem (%).

Você pode exportar e importar uma configuração de aplicativo protegida por senha. Um arquivo de configuração criado pela exportação de uma configuração de aplicativo protegida contém a soma de verificação de senha e o valor do modificador usado para preencher a cadeia de caracteres de senha.

Não altere 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 totalmente bloqueado.

Para proteger o acesso às funções do Kaspersky Embedded Systems Security for Windows:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados**. Selecione o grupo de administração com os dispositivos protegidos cujas configurações de aplicativo deseja configurar.

2. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações de política para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra as propriedades da **<Nome da política>** pelo menu de contexto.

   - Se quiser definir as configurações do aplicativo para um único dispositivo protegido, abra as configurações necessárias na janela **Configurações do aplicativo** do Kaspersky Security Center.

3. Na seção **Configurações do aplicativo** da guia **Segurança e confiabilidade**, 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 a senha que deseja utilizar para proteger o acesso às funções do Kaspersky Embedded Systems Security for Windows.

6. No campo **Confirmar senha**, insira a senha novamente.

7. Clique no botão **OK**.

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

Esta senha não pode ser recuperada. A perda da senha resultará na perda total do controle do aplicativo. Além disso, será impossível desinstalar o aplicativo do dispositivo protegido.

Você pode redefinir a senha a qualquer momento. Para isso, desmarque a caixa **Aplicar proteção de senha** e salve as alterações. A proteção por senha será desativada e a soma de verificação da senha antiga será removida. Repita o processo de criação da senha com uma senha nova.

Gerenciamento de permissões de acesso por meio do Console do Aplicativo

Nesta seção, saiba como navegar pela interface do Console do Aplicativo e definir permissões de acesso em um dispositivo protegido.

Configurando permissões de acesso para gerenciar o Kaspersky Embedded Systems Security for Windows e o Kaspersky Security Service

É possível editar a lista de usuários e grupos de usuário com permissão para acessar as funções do Kaspersky Embedded Systems Security for Windows e gerenciar o Kaspersky Security Service. Também é possível editar as permissões de acesso desses usuários e grupos de usuário.

Para adicionar ou remover um usuário ou grupo da lista:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Suplementar**, execute uma das seguintes etapas:
   - Clique no botão **Configurações** na subseção **Permissões de acesso do usuário para gerenciamento do aplicativo** caso queira editar a lista de usuários com permissões de acesso para gerenciar as funções do Kaspersky Embedded Systems Security for Windows.
   - Clique no botão **Configurações** na subseção **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service** caso queira editar a lista de usuários com permissões de acesso para gerenciar o Kaspersky Security Service.

     A janela **Permissões para** o **Kaspersky Embedded Systems Security 3.3 for Windows** é exibida.
5. 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 ao qual 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**.
6. 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 for Windows ou o Kaspersky Security Service:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Suplementar**, execute uma das seguintes etapas:

- Clique no botão **Configurações** na subseção **Permissões de acesso do usuário para gerenciamento do aplicativo** caso queira editar a lista de usuários com permissões de acesso para gerenciar as funções do Kaspersky Embedded Systems Security for Windows.

- Clique no botão **Configurações** na subseção **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service** caso queira editar a lista de usuários com permissões de acesso para gerenciar o aplicativo pelo Kaspersky Security Service.

  A janela **Permissões para** o **Kaspersky Embedded Systems Security for Windows** é exibida.

5. Na janela exibida, na lista **Grupo ou nomes de usuário**, selecione o usuário ou grupo de usuários de quem você deseja alterar as permissões.

6. Na seção **Permissões para <Usuário (Grupo)>**, selecione as caixas de seleção **Permitir** ou **Negar** para os seguintes níveis de acesso:

   - **Controle total**: conjunto completo de permissões para gerenciar o Kaspersky Embedded Systems Security for Windows ou o Kaspersky Security Service.

   - **Ler**:

     - As seguintes permissões para gerenciar o Kaspersky Embedded Systems Security for Windows: **Recuperar estatísticas**, **Ler configurações**, **Ler registros** e **Permissões de leitura**.

     - As seguintes permissões para gerenciar o Kaspersky Security Service: **Ler as configurações de serviço**, **Solicitar status 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 for Windows, exceto **Permissões de edição**.

     - As seguintes permissões para gerenciar o Kaspersky Security Service: **Modificar configurações do serviço**, **Permissões de leitura**.

   - **Permissões especiais**: as seguintes permissões para gerenciar o Kaspersky Security Service: **Inicialização do serviço**, **Parar serviço**, **Pausar/retomar serviço**, **Permissões de leitura**, **Solicitações de serviço definidos pelo usuário**.

7. Para configurar permissões avançadas para um usuário ou grupo (**Permissões especiais**), clique no botão **Avançado**.

   a. Na janela exibida **Configurações avançadas de segurança para** o **Kaspersky Embedded Systems Security for Windows**, selecione o usuário ou grupo desejado.

   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 ao lado das funções que deseja permitir ou bloquear para o usuário ou grupo selecionado.

   e. Clique no botão **OK**.

   f. Na janela **Configurações de segurança avançadas para** o **Kaspersky Embedded Systems Security for Windows**, clique em **OK**.

8. Na janela **Permissões para** o **Kaspersky Embedded Systems Security for Windows**, clique no botão **Aplicar**.

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

Acesso protegido por senha às funções do Kaspersky Embedded Systems Security for Windows

Você pode restringir o acesso ao gerenciamento do aplicativo e aos serviços registrados configurando permissões de usuário. Também é possível estabelecer uma proteção por senha nas configurações do Kaspersky Embedded Systems Security for Windows para proteção adicional de operações críticas.

O Kaspersky Embedded Systems Security for Windows solicita uma senha quando você tenta acessar as seguintes funções do aplicativo:

- conectar-se ao Console do Aplicativo;
- desinstalar o Kaspersky Embedded Systems Security for Windows;
- modificar componentes do Kaspersky Embedded Systems Security for Windows;
- executar comandos da linha de comando.

A interface do Kaspersky Embedded Systems Security for Windows disfarça a senha especificada na tela. O Kaspersky Embedded Systems Security for Windows armazena a senha como uma soma de verificação calculada quando a senha é digitada.

O Kaspersky Embedded Systems Security for Windows não verifica o nível de segurança da senha e não bloqueia a entrada de senha após várias tentativas com falha.

Ao criar uma senha, é recomendado atender às seguintes condições:

- A senha não conter o nome da conta ou o nome do computador.
- A senha ter pelo menos oito caracteres.
- A senha conter caracteres que correspondam a pelo menos três das seguintes categorias:
  - letras latinas maiúsculas (A-Z);
  - letras latinas minúsculas (a-z);
  - números (0-9);
  - símbolos de ponto de exclamação (!), cifrão ($), sinal de cardinal (#) e sinal de porcentagem (%).

Você pode exportar e importar uma configuração de aplicativo protegida por senha. Um arquivo de configuração criado pela exportação de uma configuração de aplicativo protegida contém a soma de verificação de senha e o valor do modificador usado para preencher a cadeia de caracteres de senha.

Não altere 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 totalmente bloqueado.

Para proteger o acesso às funções do Kaspersky Embedded Systems Security for Windows:

1. Na árvore do Console do Aplicativo, selecione o node **Kaspersky Embedded Systems Security for Windows** e execute uma das seguintes ações:

   - Clique no link **Propriedades do aplicativo** no painel de detalhes do node.
   - Selecione **Propriedades** no cardápio de contexto do node.

   A janela **Configurações do aplicativo** é exibida.

2. Na guia **Segurança e confiabilidade** na seção **Configurações de proteção de senha**, marque a caixa de seleção **Aplicar proteção de senha**.

   Os campos **Senha** e **Confirmar senha** ficam ativos.

3. No campo **Senha**, insira a senha que deseja utilizar para proteger o acesso às funções do Kaspersky Embedded Systems Security for Windows.

4. No campo **Confirmar senha**, insira a senha novamente.

5. Clique no botão **OK**.

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 dispositivo protegido.

Você pode redefinir a senha a qualquer momento. Para isso, desmarque a caixa **Aplicar proteção de senha** e salve as alterações. A proteção por senha será desativada e a soma de verificação da senha antiga será removida. Repita o processo de criação da senha com uma senha nova.

Gerenciamento de permissões de acesso por meio do Plug-in da Web

Nesta seção, saiba como navegar pela interface do Plug-in da Web e definir permissões de acesso para um ou todos os dispositivos protegidos na rede.

Configurando permissões de acesso para o Kaspersky Embedded Systems Security for Windows e o Kaspersky Security Service

Para configurar as permissões de acesso para um usuário ou grupo, é necessário especificar a sequência do descritor de segurança usando a linguagem de definição do descritor de segurança (SDDL). Para obter informações detalhadas sobre a sequência do descritor de segurança, acesse o site da Microsoft.

Para configurar as permissões de acesso para um usuário ou grupo:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos → Políticas e perfis**.

2. Clique no nome da política que você quer configurar.

3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.

4. Selecione a seção **Suplementar**.

5. Execute uma das seguintes ações:

   - Clique no botão **Configurações** na subseção **Permissões de acesso do usuário para gerenciamento do aplicativo** caso queira editar a lista de usuários com permissões de acesso para gerenciar as funções do Kaspersky Embedded Systems Security for Windows.

   - Clique no botão **Configurações** na subseção **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service** caso queira editar a lista de usuários com permissões de acesso para gerenciar o Kaspersky Security Service.

6. Adicione um usuário ou grupo especificando a sequência do descritor de segurança na janela **Permissões de acesso do usuário para gerenciamento do aplicativo** ou **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service**.

7. Clique no botão **OK**.

Acesso protegido por senha às funções do Kaspersky Embedded Systems Security for Windows

Você pode restringir o acesso ao gerenciamento do aplicativo e aos serviços registrados configurando permissões de usuário. Também é possível estabelecer uma proteção por senha nas configurações do Kaspersky Embedded Systems Security for Windows para proteção adicional de operações críticas.

O Kaspersky Embedded Systems Security for Windows solicita uma senha quando você tenta acessar as seguintes funções do aplicativo:

- conectar-se ao Console do Aplicativo;

- desinstalar o Kaspersky Embedded Systems Security for Windows;

- modificar componentes do Kaspersky Embedded Systems Security for Windows;

- executar comandos da linha de comando.

A interface do Kaspersky Embedded Systems Security for Windows disfarça a senha especificada na tela. O Kaspersky Embedded Systems Security for Windows armazena a senha como uma soma de verificação calculada quando a senha é digitada.

O Kaspersky Embedded Systems Security for Windows não verifica o nível de segurança da senha e não bloqueia a entrada de senha após várias tentativas com falha.

Ao criar uma senha, é recomendado atender às seguintes condições:

- A senha não conter o nome da conta ou o nome do computador.

- A senha ter pelo menos oito caracteres.

- A senha conter caracteres que correspondam a pelo menos três das seguintes categorias:
  - letras latinas maiúsculas (A-Z);
  - letras latinas minúsculas (a-z);
  - números (0-9);
  - símbolos de ponto de exclamação (!), cifrão ($), sinal de cardinal (#) e sinal de porcentagem (%).

Você pode exportar e importar uma configuração de aplicativo protegida por senha. Um arquivo de configuração criado pela exportação de uma configuração de aplicativo protegida contém a soma de verificação de senha e o valor do modificador usado para preencher a cadeia de caracteres de senha.

Não altere 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 totalmente bloqueado.

Para proteger o acesso às funções do Kaspersky Embedded Systems Security for Windows:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Configurações do aplicativo**.
5. Na seção **Segurança e confiabilidade**, clique no botão **Configurações**.
6. Na seção **Configurações de proteção de senha**, marque a caixa de seleção **Aplicar proteção de senha**.
7. No campo **Senha**, insira a senha que deseja utilizar para proteger o acesso às funções do Kaspersky Embedded Systems Security for Windows.
8. Clique no botão **OK**.

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

Esta senha não pode ser recuperada. A perda da senha resultará na perda total do controle do aplicativo. Além disso, será impossível desinstalar o aplicativo do dispositivo protegido.

Você pode redefinir a senha a qualquer momento. Para isso, desmarque a caixa **Aplicar proteção de senha** e salve as alterações. A proteção por senha será desativada e a soma de verificação da senha antiga será removida. Repita o processo de criação da senha com uma senha nova.

Proteção de Arquivos em Tempo Real

Esta seção contém informações sobre a tarefa de Proteção de Arquivos em Tempo Real e como configurá-la.

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 for Windows verifica os seguintes objetos do dispositivo protegido quando eles são acessados:

- Objetos do sistema operacional.
- Fluxos de dados alternativos do NTFS.
- Registros mestre de inicialização e setores de inicialização em discos rígidos locais e dispositivos externos.

Quando um aplicativo grava ou lê um arquivo no dispositivo protegido, o Kaspersky Embedded Systems Security for Windows intercepta esse arquivo, verifica se existem ameaças, e, se uma ameaça for detectada, ele executa uma ação padrão ou uma ação especificada pelo usuário: ele tenta desinfetá-lo, movê-lo para a Quarentena ou o exclui-lo. Antes da desinfecção ou exclusão, o Kaspersky Embedded Systems Security for Windows salvará uma cópia criptografada do arquivo fonte na pasta de Backup.

O Kaspersky Embedded Systems Security for Windows também detecta malware em processos executados sob o subsistema Windows para Linux®. Para esses processos, a tarefa de Proteção de Arquivos em Tempo Real aplica a ação definida pela configuração atual.

Sobre o escopo de proteção da tarefa e configurações de segurança

Por padrão, a tarefa de Proteção de Arquivos em Tempo Real protege todos os objetos do sistema de arquivos do dispositivo. Se não houver requisito de segurança para proteger todos os objetos do sistema de arquivos ou se você deseja excluir qualquer objeto do escopo de tarefa, é possível limitar o escopo da proteção.

No Console do Aplicativo, o escopo da proteção é exibido em uma árvore ou lista dos recursos de arquivos do dispositivo que o Kaspersky Embedded Systems Security for Windows pode monitorar. Por padrão, os recursos de arquivos de rede do dispositivo são exibidos em uma lista.

No Plug-in de Administração, apenas a exibição de lista está disponível.

Para exibir recursos de arquivos de rede em uma árvore no Console do Aplicativo,

abra a lista suspensa na seção superior esquerda da janela **Configurações do escopo da proteção** e selecione **Visualização em árvore**.

Independentemente de os recursos de arquivo do dispositivo protegido serem exibidos como uma lista ou uma árvore, os ícones do node têm os seguintes significados:

☑ O nó é incluído no escopo de proteção.

☐ O nó é excluído a partir do escopo de proteção.

Pelo menos um dos nodes secundários deste nó é excluído do escopo da proteção, ou as configurações de segurança do(s) node(s) secundário(s) são diferentes das do node principal (somente para o modo de visualização em árvore).

O ícone é exibido se todos os nodes secundários forem selecionados, mas se o node principal não for selecionado. Nesse caso, as alterações na composição dos arquivos e pastas do node principal são desconsideradas automaticamente quando o escopo da proteção para o node secundário selecionado é criado.

Usando o Console do Aplicativo, você também pode adicionar unidades virtuais ao escopo da proteção. Os nomes dos nodes virtuais são exibidos em azul.

Configurações de segurança

As configurações de segurança de tarefas podem ser definidas como configurações em comum para todos os nodes ou itens incluídos no escopo da proteção ou como configurações distintas para cada nó ou item na árvore ou lista de recursos de arquivos do dispositivo.

As configurações de segurança definidas para o node principal selecionado são automaticamente aplicadas a todos os seus nós filhos. As configurações de segurança do node principal não são aplicadas a nós filhos configurados separadamente.

As configurações de um escopo de proteção selecionado podem ser definidas usando um dos seguintes métodos:

- Seleção de um dos três níveis de segurança predefinidos.
- Definição manual das configurações de segurança para os nodes ou itens selecionados na árvore ou lista de recursos de arquivo (o nível de segurança é alterado para **Personalizado**).

Um conjunto de configurações de um nó ou item pode ser salvo em um modelo para ser aplicado posteriormente a outros nodes ou itens.

Sobre escopo da proteção virtual

O Kaspersky Embedded Systems Security for Windows pode verificar não apenas as pastas e arquivos existentes em discos rígidos e unidades removíveis, mas também unidades criadas dinamicamente no dispositivo protegido por vários aplicativos e serviços.

Se todos os objetos do dispositivo forem incluídos no escopo da proteção, esses nós dinâmicos serão incluídos automaticamente no escopo da proteção. No entanto, caso deseje especificar valores especiais para as configurações de segurança desses nós dinâmicos ou caso tenha selecionado apenas uma parte do dispositivo para a proteção, para incluir unidades, arquivos ou pastas virtuais no escopo da proteção, primeiro será necessário criá-los no Console do Aplicativo, ou seja, especificar o escopo da proteção virtual. As unidades, os arquivos e as pastas criados existirão apenas no Console do Aplicativo e não na estrutura de arquivos do dispositivo protegido.

Se, ao criar um escopo da proteção, todas as subpastas ou arquivos forem selecionados sem que a pasta pai seja selecionada, todas as pastas ou os arquivos virtuais que são exibidos nela não serão incluídos automaticamente no escopo da proteção. "Cópias virtuais" deles devem ser criadas no Console do Aplicativo e adicionadas ao escopo da proteção.

Escopos da proteção predefinidos

A árvore ou lista de recursos de arquivos exibe os nodes aos quais você tem acesso à leitura com base nas configurações de segurança definidas no Microsoft Windows.

O Kaspersky Embedded Systems Security for Windows abrange os seguintes escopos de proteção predefinidos:

- **Discos rígidos locais**. O Kaspersky Embedded Systems Security for Windows protege arquivos nos discos rígidos do dispositivo.
- **Unidades removíveis**. O Kaspersky Embedded Systems Security for Windows protege arquivos em dispositivos externos, como CDs ou drives removíveis. É possível incluir ou excluir do escopo da proteção todos os drives removíveis, discos individuais, pastas ou arquivos individuais.
- **Rede**. O Kaspersky Embedded Systems Security for Windows verifica os arquivos gravados em pastas de redes ou lidos nelas por aplicativos em execução no dispositivo. O Kaspersky Embedded Systems Security for Windows não protege os arquivos quando eles são acessados por aplicativos de outros dispositivos protegidos.
- **Unidades virtuais**. Pastas e arquivos virtuais e unidades que temporariamente conectadas ao dispositivo 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 um comando SUBST não são exibidas na árvore de recursos de arquivos do dispositivo protegido no Console do Aplicativo. Para incluir objetos da unidade virtual no escopo da proteção, inclua a pasta do dispositivo associada à unidade virtual no escopo da proteção.

As unidades de rede conectadas também não serão exibidas na lista de recursos de arquivos do dispositivo protegido. 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.

Sobre níveis de segurança predefinidos

Um dos seguintes níveis de segurança predefinidos para os nós selecionados na árvore ou na lista de recursos de arquivo do dispositivo protegido pode ser aplicado: **Desempenho máximo**, **Recomendado** e **Proteção máxima**. Cada um desses níveis contém o próprio conjunto de configurações de segurança predefinido (veja a tabela abaixo).

Desempenho máximo

O nível de segurança **Desempenho máximo** é recomendado se a rede tiver medidas de segurança adicionais nos dispositivos protegidos, como firewalls e políticas de segurança existentes, além de usar o Kaspersky Embedded Systems Security for Windows nos dispositivos protegidos.

Recomendado

O nível de segurança **Recomendado** assegura a melhor combinação de impacto de proteção e desempenho nos dispositivos. Os especialistas da Kaspersky recomendam esse nível como adequado para proteger dispositivos 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 de dispositivos.

Somente notificações

O nível de segurança **Somente notificações** é recomendado caso haja muitos computadores potencialmente infectados na rede corporativa, e bloqueá-los poderia interromper significativamente a operação da organização.

Níveis de segurança predefinidos e valores de configurações correspondentes

Opções	Nível de segurança			
	Desempenho máximo	**Recomendado**	**Proteção máxima**	**Somente notificações**
Proteção de objetos	Por extensão	Por formato	Por formato	Por formato
Proteger somente arquivos novos e modificados	Ativado	Ativado	Desativado	Ativado
Ação a ser executada em objetos infectados e outros	Bloquear acesso e desinfectar. Remover, caso a desinfecção falhe	Bloquear acesso e executar a ação recomendada pelos especialistas da Kaspersky	Bloquear acesso e desinfectar. Remover, caso a desinfecção falhe	Somente notificações
Ação a ser executada em objetos possivelmente infectados	Bloquear acesso e colocar na quarentena	Bloquear acesso e executar a ação recomendada pelos especialistas da Kaspersky	Bloquear acesso e colocar na quarentena	Somente notificações
Os objetos críticos do sistema são arquivos necessários para a operação do sistema operacional e do Kaspersky Embedded Systems Security for Windows. Esses arquivos não podem ser excluídos. Os processos associados a esses objetos não podem ser encerrados.				
Excluir arquivos	Não	Não	Não	Não
Não detectar	Não	Não	Não	Não
Parar a verificação se	60 s	60 s	60 s	60 s

demorar mais que (s)				
Não verificar objetos compostos com mais de (MB)	8 MB	8 MB	Não definido	8 MB
Verificar fluxos NTFS alternativos	Sim	Sim	Sim	Sim
Verificar setores de inicialização do disco e MBR	Sim	Sim	Sim	Sim
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	• Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* * Somente objetos novos e modificados
Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado	Não	Não	Sim	Não

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.

Extensões de arquivos verificadas por padrão na tarefa de Proteção de Arquivos em Tempo Real

O Kaspersky Embedded Systems Security for Windows verifica arquivos das seguintes extensões por padrão:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*

- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*
- *.exe*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*
- *ico;*
- *inf;*

- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*

- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*

- *ov?;*
- *pp?;*
- *vs?;*
- *xl?.*

Configurações padrão da tarefa de Proteção de arquivos em tempo real

Por padrão, a tarefa de Proteção de Arquivos em Tempo Real usa as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Configurações padrão da tarefa de Proteção de arquivos em tempo real

Configuração	Valor padrão	Descrição
escopo da proteção	O dispositivo protegido inteiro, excluindo unidades virtuais.	Use esta opção para alterar o escopo de proteção.
Configurações de segurança	As configurações comuns de todo o escopo da proteção correspondem ao nível de segurança **Recomendado**.	Para os nodes selecionados na lista ou na árvore de recursos de arquivos do dispositivo protegido, é possível: • Selecionar um nível de segurança predefinido diferente • Alterar manualmente as configurações de segurança É possível salvar um grupo de configurações de segurança para um nó selecionado como um modelo para ser usado posteriormente para outro node.
Modo de proteção dos objetos	**Modo inteligente**	Use esta opção para o modo de proteção, ou seja, definir o tipo de tentativas de acesso pelas quais o Kaspersky Embedded Systems Security for Windows verifica 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.	Use esta opção para melhorar a proteção do dispositivo com o uso do serviço na nuvem da Kaspersky Security Network (disponível caso a Declaração da KSN seja aceita).
Programação de inicialização da tarefa	Na inicialização do aplicativo.	Use esta opção para configurar no início de tarefas agendadas.
Bloquear o acesso a recursos de rede compartilhados para sessões que exibem atividade maliciosa	Não aplicado.	Use esta opção para bloquear a sessão atual e adicionar o IP do host ou a LUID do host para a qual a atividade maliciosa foi detectada na seção armazenamento de hosts bloqueados.

Iniciar a verificação de áreas críticas quando uma infecção ativa for detectada	Aplicada.	Quando a infecção ativa for detectada, o Kaspersky Embedded Systems Security for Windows criará e iniciará uma tarefa temporária de Verificação de Áreas Críticas.

Gerenciamento da tarefa de Proteção de Arquivos em Tempo Real por meio do Plug-in de Administração

Nesta seção, saiba como navegar pela interface do Plug-in de Administração e definir configurações de tarefa para um ou todos os dispositivos protegidos na rede.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das definições de política para a tarefa de proteção de Arquivos em Tempo Real

Para abrir as definições da tarefa de Proteção de Arquivos em Tempo Real por meio da política do Kaspersky Security Center:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Proteção do Computador em Tempo Real**.
6. Clique em **Configurações** na subseção **Proteção de Arquivos em Tempo Real**.

   A janela **Proteção de arquivos em tempo real** é exibida.

Se um dispositivo protegido estiver sendo gerenciado por uma política ativa do Kaspersky Security Center e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas por meio do Console do Aplicativo.

Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real

Para abrir as configurações da tarefa de Proteção de Arquivos em Tempo Real para um único dispositivo da rede:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Dispositivos**.
4. Abra a janela **Propriedades: <Nome do dispositivo protegido>** usando uma das seguintes maneiras:
   - Clique duas vezes no nome do dispositivo protegido.
   - Abra o menu de contexto do nome do dispositivo protegido e selecione o item **Propriedades**.

   A janela **Propriedades: <Nome do dispositivo protegido>** é exibida.
5. Na seção **Tarefas**, selecione a tarefa **Proteção de Arquivos em Tempo Real**.
6. Clique no botão **Propriedades**.
   A janela **Propriedades: Proteção de Arquivos em Tempo Real** é exibida.

Configuração da tarefa de Proteção de Arquivos em Tempo Real

Para configurar a tarefa de Proteção de arquivos em tempo real:

1. Abra a janela **Proteção de arquivos em tempo real**.
2. Defina as seguintes configurações da tarefa:
   - Na guia **Geral**:
     - Parâmetros de interceptação
     - **Analisador heurístico**
     - **Integração com outros componentes**
   - Na guia **Gerenciamento da tarefa**:
     - Configurações da programação de inicialização da tarefa.
3. Selecione a guia **Escopo da proteção** e faça o seguinte:
   - Clique no botão **Adicionar** ou **Editar** para editar o escopo da proteção.
     - Na janela aberta, escolha o que você deseja incluir no escopo da proteção da tarefa:
       - **Escopo predefinido**
       - **Disco, pasta ou local de rede**
       - **Arquivo**

- Selecione um dos níveis de segurança predefinidos ou defina manualmente as configurações de proteção.

4. Clique no botão **OK** na janela **Proteção de arquivos em tempo real**.

O Kaspersky Embedded Systems Security for Windows aplica imediatamente as novas configurações à tarefa em execução. A data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Seleção do 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 especificar o tipo de tentativas de acesso pelas quais o Kaspersky Embedded Systems Security for Windows verifica objetos.

O valor da configuração **Modo de proteção dos objetos** se aplica a todo o escopo da proteção 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. Abra a janela **Proteção de arquivos em tempo real**.

2. Na janela exibida, abra a guia **Geral** e selecione o modo de proteção que deseja estabelecer:

   - **Modo inteligente**
   - **Ao acessar e modificar**
   - **Ao acessar**
   - **Ao executar**
   - **Análise profunda de processos sendo inicializados (a inicialização do processo é bloqueada até que a análise termine)**

3. Clique no botão **OK**.

O modo de proteção selecionado entrará em vigor.

Configuração do Analisador Heurístico e integração com outros componentes do aplicativo

Para iniciar a tarefa de Uso da KSN, você deve aceitar a Declaração da Kaspersky Security Network.

Para configurar o Analisador Heurístico e a integração com outros componentes:

1. Abra a janela **Proteção de arquivos em tempo real**.

2. Na guia **Geral**, selecione ou desmarque a caixa de seleção **Usar o analisador heurístico**

3. Se necessário, ajuste o nível da análise usando o controle deslizante.

4. Na seção **Integração com outros componentes**, defina as seguintes configurações:

   - Selecione ou desmarque a caixa de seleção **Aplicar Zona Confiável**.
   - Selecione ou desmarque a caixa de seleção **Usar a KSN para proteção**.

     A caixa de seleção **Enviar dados dos arquivos verificados** deve estar selecionada na configuração da tarefa de Uso da KSN.

   - Selecione ou desmarque a caixa de seleção **Bloquear o acesso a recursos de rede compartilhados para sessões que exibem atividade maliciosa**.
   - Marque ou desmarque a caixa de seleção **Iniciar a verificação de áreas críticas quando uma infecção ativa for detectada**.

5. Clique no botão **OK**.

As configurações de tarefa definidas são aplicadas imediatamente a uma tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

Programação de tarefas

É possível programar tarefas locais do sistema e tarefas personalizadas no Console do Aplicativo. Não é possível programar tarefas de grupo no Console do Aplicativo.

Para programar tarefas de grupo utilizando o Plug-in de Administração:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados**.
2. Selecione o grupo ao qual o dispositivo protegido pertence.
3. No painel de resultados, selecione a guia **Tarefas**.
4. Abra a janela **Propriedades: <Nome da tarefa>** usando uma das seguintes maneiras:

   - Clique duas vezes no nome da tarefa.
   - Abra o menu de contexto do nome da tarefa e selecione o item Propriedades.

5. Selecione a seção **Agendamento**.
6. No bloco **Configurações de agendamento**, marque a caixa de seleção **Executar de acordo com o agendamento**.

   Os campos com configurações de programação para as tarefas de Verificação por Demanda e de Atualização estarão indisponíveis caso a programação dessas tarefas seja bloqueada por uma política do Kaspersky Security Center.

7. 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 nos quais a tarefa será iniciada (por padrão, as tarefas são executadas nas segundas-feiras).
- **Ao iniciar o aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security for Windows.
- **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 quando a programação inicia.

Depois de programar a hora e data de início e a frequência da tarefa, a hora estimada para a próxima execução é exibida.

Acesse a guia **Agendamento** e abra a janela **Configurações de tarefa**. No campo **Próxima execução** na parte superior da janela, a hora de inicialização estimada é exibida. Cada vez que a janela é aberta, essa hora de início estimada é atualizada e exibida.

O campo **Próxima execução** exibe o valor **Bloqueado pela política** caso as configurações de política ativa do Kaspersky Security Center proíbam a execução de tarefas locais do sistema programadas.

8. 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, nos campos à direita, insira o número máximo de horas e minutos da execução da tarefa.

  b. Marque a caixa de seleção **Pausar de** e, nos campos à direita, insira os valores iniciais e finais de um intervalo de tempo menor que 24 horas durante o qual a execução da tarefa será pausada.

- No bloco **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 **Randomizar a hora de início da tarefa no intervalo de** e especifique um valor em minutos.

9. Clique no botão **OK**.

10. Clique no botão **Aplicar** para salvar as configurações de início da tarefa.

Caso queira definir as configurações do aplicativo para uma única tarefa usando o Kaspersky Security Center, acesse a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center".

Criação e configuração do escopo de proteção da tarefa

Para criar e configurar o escopo de proteção da tarefa por meio do Kaspersky Security Center:

1. Abra a janela **Proteção de arquivos em tempo real**.

2. Selecione a guia **Escopo da proteção**.

   Todos os itens já protegidos pela tarefa são listados na tabela **Escopo da proteção**.

3. Clique no botão **Adicionar** para adicionar um novo item à lista.

   A janela **Adicionar objetos ao escopo da proteção** será aberta.

4. Selecione um tipo de objeto para adicioná-lo a um escopo de proteção:

   - **Escopo predefinido** - para incluir um dos escopos predefinidos no escopo da proteção no dispositivo. Em seguida, na lista suspensa, selecione o escopo da proteção desejado.
   - **Disco, pasta ou local de rede** - para incluir unidade individual, pasta ou um objeto de rede no escopo da proteção. Em seguida, selecione o escopo da proteção desejado clicando no botão **Procurar**.
   - **Arquivo** - para incluir um arquivo individual no escopo da proteção. Em seguida, selecione o escopo da proteção desejado clicando no botão **Procurar**.

     Não é possível adicionar um objeto a um escopo da proteção se ele já tiver sido adicionado como uma exclusão do escopo da proteção.

5. Para excluir itens individuais do escopo da proteção, desmarque as caixas de seleção ao lado dos nomes desses itens ou siga as etapas a seguir:

   a. Abra o menu de contexto do escopo da verificação clicando nele com o botão direito.

   b. No menu de contexto, selecione a opção **Adicionar exclusão**.

   c. Na janela **Adicionar exclusão**, selecione um tipo de objeto que deseja adicionar como uma exclusão do escopo da proteção seguindo o procedimento usado ao adicionar um objeto ao escopo da proteção.

6. Para modificar o escopo da proteção ou uma exclusão existente, selecione a opção **Editar escopo** no menu de contexto do escopo de proteção desejado.

7. Para ocultar um escopo da proteção adicionado anteriormente ou uma exclusão na lista de recursos de arquivos de rede, selecione a opção **Remover escopo** no menu de contexto do escopo da proteção desejado.

Um escopo da proteção é removido do escopo da tarefa de Proteção de arquivos em tempo real ao ser removido da lista de recursos de arquivos de rede.

8. Clique no botão **OK**.

A janela Configurações do escopo da proteção é fechada. As configurações especificadas são salvas.

A tarefa **Proteção de Arquivos em Tempo Real** pode ser iniciada se pelo menos um dos nós de recursos de arquivos do dispositivo for incluído em um escopo da proteção.

Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda

É possível aplicar um dos seguintes três níveis de segurança predefinidos para um nó selecionado na lista de recursos de arquivos do dispositivo: **Desempenho máximo**, **Recomendado** e **Proteção máxima**.

Para selecionar um dos níveis de segurança predefinidos:

1. A janela **Propriedades: Proteção de Arquivos em Tempo Real**.
2. Selecione a guia **Escopo da proteção**.
3. Na lista do dispositivo protegido, selecione um item incluído no escopo da proteção para definir um nível de segurança predefinido.
4. Clique no botão **Configurar**.

   A janela **Configurações de Proteção de Arquivos em Tempo Real** é exibida.
5. Na guia **Nível de segurança**, selecione o nível de segurança a ser aplicado.

   A janela exibe a lista de configurações de segurança correspondentes ao nível de segurança selecionado.
6. Clique no botão **OK**.
7. Clique no botão **OK** na janela **Propriedades: Proteção de Arquivos em Tempo Real**.

   As configurações de tarefa definidas serão salvadas e aplicadas imediatamente à uma tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

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**.

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 itens individuais na lista de recursos de arquivos ou nós da árvore do dispositivo.

Para definir as configurações de segurança do node selecionado manualmente:

1. Abra a janela **Proteção de arquivos em tempo real**.
2. Na guia **Escopo da proteção**, selecione o node cujas configurações de segurança você deseja definir e clique em **Configurar**.

   A janela **Configurações de Proteção de Arquivos em Tempo Real** é exibida.
3. Na guia **Nível de segurança**, clique no botão **Configurações** para personalizar a configuração.
4. É possível definir configurações de segurança personalizadas para o node selecionado, de acordo com os seus requisitos:
   - Configurações gerais
   - Ações
   - Desempenho
5. Clique no botão **OK** na janela **Proteção de arquivos em tempo real**.

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**.
2. Abra a guia **Geral**.
3. No bloco **Proteção de objetos**, especifique os tipos de objetos que deseja incluir no escopo da proteção:
   - **Todos os objetos**
   - **Objetos verificados por formato**
   - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**
   - **Objetos verificados pela lista de extensões especificada**
   - **Verificar setores de inicialização do disco e MBR**
   - **Verificar fluxos NTFS alternativos**
4. No grupo **Desempenho**, marque ou desmarque a caixa de seleção **Proteger somente arquivos novos e modificados**.

   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. No bloco **Proteção de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da proteção:

   - **Todos** / **Apenas novos arquivos compactados**
   - **Todos** / **Apenas novos arquivos compactados SFX**
   - **Todos** / **Apenas novos bancos de dados de e-mail**
   - **Todos** / **Apenas novos objetos compactados**
   - **Todos** / **Apenas novos e-mails sem formatação**
   - **Todos** / **Apenas novos objetos OLE incorporados**

6. Clique no botão **Salvar**.

A nova configuração de tarefa será salva.

Configurar ações

Para configurar ações em objetos infectados e outros objetos detectados durante a tarefa de Proteção de Arquivos em Tempo Real:

1. Abra a janela **Configurações de Proteção de Arquivos em Tempo Real**.
2. Selecione a guia **Ações**.
3. Selecione a ação a ser executada em objetos infectados e outros objetos detectados:

   - **Somente notificações**.
   - **Bloquear o acesso**.
   - **Executar ação adicional**.
     Selecionar ação da lista suspensa:
     - **Desinfectar**.
     - **Desinfectar. Remover se a desinfecção falhar**Remover, caso a desinfecção falhe.
     - **Remover**.
     - **Recomendado**.

4. Selecione a ação a ser executada em objetos possivelmente infectados:

   - **Somente notificações**.
   - **Bloquear o acesso**.
   - **Executar ação adicional**
     Selecionar ação da lista suspensa:

- **Quarentena**.
- **Remover**.
- **Recomendado**.

5. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:
   a. Desmarque ou marque a caixa **Executar ações dependendo do tipo de objeto detectado**.
   b. Clique no botão **Configurações**.
   c. Na janela que se abre, selecione uma ação primária e uma ação secundária (a ser executada se a ação primária falhar) para cada tipo de objeto detectado.
   d. Clique no botão **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 o objeto incorporado**.
7. Clique no botão **Salvar**.

A nova configuração de tarefa será salva.

Configurar o desempenho

Para definir configurações de desempenho da tarefa de Proteção de Arquivos em Tempo Real:

1. Abra a janela **Configurações de Proteção de Arquivos em Tempo Real**.
2. Selecione a guia **Desempenho**.
3. No bloco **Exclusões**:
   - Desmarque ou marque a caixa de seleção **Excluir arquivos**.
   - Desmarque ou marque a caixa **Não detectar**.
   - Clique no botão **Editar** de cada configuração para adicionar exclusões.
4. No bloco **Configurações avançadas**:
   - **Parar a verificação se demorar mais que (s)**
   - **Não verificar objetos compostos com mais de (MB)**
   - **Usar a tecnologia iSwift**
   - **Usar a tecnologia iChecker**

Gerenciamento da tarefa de Proteção de Arquivos em Tempo Real por meio do Console do Aplicativo

Nesta seção, aprenda a navegar pela interface do Console do Aplicativo e definir as configurações de tarefa em um dispositivo protegido.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real

Para abrir a janela de configurações gerais da tarefa:

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó filho **Proteção de Arquivos em Tempo Real**.
3. Clique no link **Propriedades** no painel de resultados.
   A janela **Configurações de tarefa** é aberta.

Abertura das configurações do escopo da tarefa de Proteção de Arquivos em Tempo Real

Para abrir a janela Configurações do escopo da proteção para a tarefa de Proteção de Arquivos em Tempo Real:

1. Na árvore do Console do Aplicativo, expanda o node **Proteção do Computador em Tempo Real**.
2. Selecione o node secundário **Proteção de Arquivos em Tempo Real**.
3. Clique no link **Configurar o escopo da proteção** no painel de resultados.
   A janela **Configurações do escopo da proteção** é exibida.

Configuração da tarefa de Proteção de Arquivos em Tempo Real

Para configurar a tarefa de Proteção de arquivos em tempo real:

1. Abra a janela **Configurações de tarefa**.
2. Na guia **Geral**, defina as seguintes configurações de tarefa:

- Modo de proteção dos objetos
- **Analisador heurístico**
- **Integração com outros componentes**

3. Nas guias **Agendamento** e **Avançado**, especifique as configurações de início programado.
4. Clique em **OK** na janela **Configurações de tarefa**.

   As configurações modificadas são salvas.
5. No painel de resultados do node **Proteção de Arquivos em Tempo Real**, clique no link **Configurar o escopo da proteção**.
6. Faça o seguinte:
   - Na árvore ou lista de recursos de arquivos do dispositivo, selecione os nodes ou itens que deseja incluir no escopo da proteção da tarefa.
   - Selecione um dos níveis de segurança predefinidos ou defina as configurações de proteção do objeto manualmente.
7. Na janela **Configurações do escopo da proteção**, clique no botão **Salvar**.

O Kaspersky Embedded Systems Security for Windows aplica imediatamente as novas configurações à tarefa em execução. A data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

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 especificar o tipo de tentativas de acesso pelas quais o Kaspersky Embedded Systems Security for Windows verifica objetos.

O valor da configuração **Modo de proteção dos objetos** se aplica a todo o escopo da proteção 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. Abra a janela **Configurações de tarefa**.
2. Na janela exibida, abra a guia **Geral** e selecione o modo de proteção que deseja estabelecer:
   - **Modo inteligente**
   - **Ao acessar e modificar**
   - **Ao acessar**
   - **Ao executar**

- **Análise profunda de processos sendo inicializados (a inicialização do processo é bloqueada até que a análise termine)**

3. Clique no botão **OK**.

O modo de proteção selecionado entrará em vigor.

Configuração do Analisador Heurístico e integração com outros componentes do aplicativo

Para iniciar a tarefa de Uso da KSN, você deve aceitar a Declaração da Kaspersky Security Network.

Para configurar o Analisador Heurístico e a integração com outros componentes:

1. Abra a janela **Configurações de tarefa**.
2. Na guia **Geral**, selecione ou desmarque a caixa de seleção **Usar o analisador heurístico**.
3. Se necessário, ajuste o nível da análise usando o controle deslizante.
4. Na seção **Integração com outros componentes**, defina as seguintes configurações:
   - Selecione ou desmarque a caixa de seleção **Aplicar Zona Confiável**.
     Clique no link **Zona Confiável** para abrir as configurações da Zona Confiável.
   - Selecione ou desmarque a caixa de seleção **Usar a KSN para proteção**.

     A caixa de seleção **Enviar dados dos arquivos verificados** deve estar selecionada na configuração da tarefa de Uso da KSN.
   - Selecione ou desmarque a caixa de seleção **Bloquear o acesso a recursos de rede compartilhados para sessões que exibem atividade maliciosa**.
   - Marque ou desmarque a caixa de seleção **Iniciar a verificação de áreas críticas quando uma infecção ativa for detectada**.
5. Clique no botão **OK**.

As configurações recém-definidas são aplicadas.

Definição das configurações da programação da tarefa

No Console do Aplicativo, é possível programar o início de tarefas locais do sistema e tarefas personalizadas. No entanto, não é possível programar o início de tarefas de grupo.

Para programar uma tarefa:

1. Abra o menu de contexto da tarefa que deseja programar.

2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é aberta.

3. Na janela exibida, na guia **Agendamento**, marque a caixa de seleção **Executar de acordo com o agendamento**.

4. Siga estas etapas para especificar as configurações de programação:

   a. No menu suspenso **Frequência**, selecione uma das seguintes opções:

   - **De hora em hora**: para executar a tarefa em intervalos medidos em horas; especifique o número de horas no campo **A cada<número>hora(s)**.
   - **Diariamente**: para executar a tarefa em intervalos diários; especifique o número de dias no campo **A cada<número>dia(s)**.
   - **Semanalmente**: para executar a tarefa em intervalos semanais; especifique o número de semanas no campo **A cada<número>semana(s) em**. Especifique os dias da semana nos quais a tarefa será iniciada (por padrão, as tarefas são executadas nas segundas-feiras).
   - **Ao iniciar o aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security for Windows.
   - **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 em que a tarefa será iniciada pela primeira vez.

   Após ter especificado a frequência de início da tarefa, a hora da primeira inicialização e a data a partir da qual a programação será aplicada, a hora estimada para a próxima inicialização da tarefa será exibida na parte superior da janela, no campo **Próxima execução**. A hora estimada da próxima execução da tarefa será atualizada e exibida sempre que você abrir a janela **Configurações de tarefa** na guia **Agendamento**.

   O campo **Próxima execução** exibe o valor **Bloqueado pela política** caso as configurações de política ativa do Kaspersky Security Center proíbam a execução de tarefas locais do sistema programadas.

5. Utilize a guia **Avançado** para especificar as seguintes configurações de programação:

   - Na seção **Configurações de interrupção de tarefa**:

     a. Marque a caixa de seleção **Duração**. Nos campos à direita, insira a duração máxima da tarefa em horas e minutos.

     b. Marque a caixa de seleção **Pausar de**. Nos campos à direita, insira quando pausar e reiniciar a tarefa (menos de 24 horas).

   - No bloco **Configurações avançadas**:

     a. Marque a caixa de seleção **Cancelar agendamento a partir de** e especifique a data de término da programação da tarefa.

b. Marque a caixa de seleção **Executar tarefas ignoradas** para inicializar as tarefas ignoradas.

c. Marque a caixa de seleção **Aleatorizar o início da tarefa dentro do intervalo de** e especifique um valor em minutos.

6. Clique no botão **OK**.

As configurações de programação da tarefa são salvas.

Criação do escopo da proteção

Esta seção fornece instruções sobre a criação e o gerenciamento de um escopo da proteção na tarefa de Proteção de Arquivos em Tempo Real.

Configuração da visualização de recursos de arquivos de rede

Para selecionar a exibição para recursos de arquivos de rede durante a definição das configurações do escopo da proteção:

1. Abra a janela **Configurações do escopo da proteção**.
2. Abra a lista suspensa na parte esquerda superior da janela e selecione uma das seguintes opções:
   - Selecione a opção **Visualização em árvore** para exibir os recursos de arquivos de rede em uma árvore.
   - Selecione a opção **Visualização em lista** para exibir os recursos de arquivos de rede em uma lista.

   Por padrão, os recursos de arquivos de rede do dispositivo protegido são exibidos em um modo de visualização em lista.
3. Clique no botão **Salvar**.

Criação do escopo da proteção

O procedimento para criar o escopo da tarefa de Proteção de Arquivos em Tempo Real depende da exibição dos recursos de arquivo de rede selecionados. É possível configurar a visualização de recursos de arquivos de rede em uma árvore ou lista (visualização padrão).

Para aplicar à tarefa as novas configurações do escopo da proteção, a tarefa de Proteção de Arquivos em Tempo real deve ser reiniciada.

Para criar um escopo da proteção usando a árvore de recursos de arquivos de rede:

1. Abra a janela **Configurações do escopo da proteção**.

2. Na seção esquerda da janela, abra a árvore de recursos de arquivos de rede para exibir todos os nodes e nós filhos.

3. Faça o seguinte:

   - Para excluir os nodes individuais do escopo da proteção, desmarque as caixas ao lado dos nomes destes nós.

   - Para incluir nós individuais no escopo da proteção, desmarque a caixa de seleção **Meu Computador** e faça o seguinte:

     - Caso queira incluir todas as unidades do mesmo tipo no escopo da proteção, marque a caixa de seleção ao lado do nome do tipo de unidades necessário. Por exemplo, para incluir todas as unidades removíveis em um dispositivo, marque a caixa de seleção **Unidades removíveis**.

     - Para incluir um disco individual de um determinado tipo no escopo da proteção, expanda o node que contém a lista de unidades desse tipo e marque a caixa ao lado do nome da unidade desejada. Por exemplo, para selecionar a unidade removível F:, expanda o nó **Unidades removíveis** e marque a caixa de seleção da unidade **F:**.

     - Se deseja incluir somente uma única pasta ou arquivo na unidade, selecione a caixa ao lado do nome daquela pasta ou arquivo.

4. Clique no botão **Salvar**.

A janela **Configurações do escopo da proteção** é fechada. As configurações especificadas são salvas.

Para criar um escopo da proteção usando a lista de recursos de arquivos de rede:

1. Abra a janela **Configurações do escopo da proteção**.

2. Para incluir nós individuais no escopo da proteção, desmarque a caixa de seleção **Meu Computador** e faça o seguinte:

   a. Abra o menu de contexto do escopo da verificação clicando nele com o botão direito.

   b. No menu de contexto do botão, selecione **Adicionar escopo da proteção**.

   c. Na janela **Adicionar escopo da proteção**, selecione um tipo de objeto para adicioná-lo ao escopo da proteção:

      - **Escopo predefinido** - para incluir um dos escopos predefinidos no escopo da proteção no dispositivo. Em seguida, na lista suspensa, selecione o escopo da proteção desejado.

      - **Disco, pasta ou local de rede** - para incluir unidade individual, pasta ou um objeto de rede no escopo da proteção. Em seguida, selecione o escopo desejado clicando no botão **Procurar**.

      - **Arquivo** - para incluir um arquivo individual no escopo da proteção. Em seguida, selecione o escopo desejado clicando no botão **Procurar**.

   Não é possível adicionar um objeto a um escopo da proteção se ele já tiver sido adicionado como uma exclusão do escopo da proteção.

3. Para excluir nós individuais do escopo da proteção, desmarque as caixas ao lado dos nomes destes nós ou siga as etapas a seguir:

a. Abra o menu de contexto do escopo da verificação clicando nele com o botão direito.

b. No menu de contexto, selecione a opção **Adicionar exclusão**.

c. Na janela **Adicionar exclusão**, selecione um tipo de objeto que deseja adicionar como uma exclusão do escopo da proteção seguindo o procedimento usado ao adicionar um objeto ao escopo da proteção.

4. Para modificar o escopo da proteção ou uma exclusão existente, selecione a opção **Editar escopo** no menu de contexto do escopo de proteção desejado.

5. Para ocultar um escopo da proteção adicionado anteriormente ou uma exclusão na lista de recursos de arquivos de rede, selecione a opção **Remover da lista** no menu de contexto do escopo da proteção desejado.

Um escopo da proteção é removido do escopo da tarefa de Proteção de arquivos em tempo real ao ser removido da lista de recursos de arquivos de rede.

6. Clique no botão **Salvar**.

A janela **Configurações do escopo da proteção** é fechada. As configurações especificadas são salvas.

A tarefa Proteção de Arquivos em Tempo Real pode ser iniciada se pelo menos um dos nodes de recursos de arquivos do dispositivo for incluído em um escopo da proteção.

Se for especificado um escopo da proteção complexo, por exemplo, se diferentes valores de segurança para configurações de vários nodes na árvore de recursos de arquivos do dispositivo forem especificados, isso poderá deixar a verificação dos objetos mais lenta quando eles forem acessados.

Incluindo objetos de rede no escopo da proteção

Unidades, pastas ou arquivos de rede podem ser adicionados ao escopo da proteção especificando seu caminho no formato UNC (Universal Naming Convention).

Você pode verificar pastas de rede na conta do sistema.

Para adicionar uma localização de rede ao escopo da proteção:

1. Abra a janela **Configurações do escopo da proteção**.

2. Abra a lista suspensa na parte esquerda superior da janela e selecione **Visualização em árvore**.

3. No menu de contexto do node **Rede**:

   - Selecione **Adicionar pasta de rede** se quiser adicionar uma pasta de rede ao escopo da proteção.

   - Selecione **Adicionar arquivo de rede** se quiser adicionar um arquivo de rede ao escopo da proteção.

4. Insira o caminho para a pasta ou arquivo de rede em formato UNC.

5. Pressione a tecla **ENTER**.

6. Marque a caixa de seleção ao lado do objeto de rede adicionado recentemente para incluí-lo no escopo da proteção.

7. Se necessário, altere as configurações de segurança do objeto de rede adicionado.

8. Clique no botão **Salvar**.

As configurações da tarefa especificadas serão salvas.

Criação de um escopo da proteção virtual

Você pode expandir o escopo da proteção/verificação adicionando unidades virtuais individuais, pastas ou arquivos somente se o escopo da proteção/verificação for apresentado como uma árvore de recursos de arquivos.

Para adicionar uma unidade virtual ao escopo da proteção:

1. Abra a janela **Configurações do escopo da proteção**.

2. Abra a lista suspensa na parte esquerda superior da janela e selecione **Visualização em árvore**.

3. Abra o menu de contexto do node **Unidades virtuais**.

4. Selecione a opção **Adicionar unidade virtual**.

5. Na lista de nomes disponíveis, selecione o nome da unidade virtual que está sendo criada.

6. Selecione a caixa ao lado da unidade para incluí-la no escopo da proteção.

7. Na janela **Configurações do escopo da proteção**, clique no botão **Salvar**.

As configurações especificadas são salvas.

Para adicionar uma pasta ou arquivo virtual ao escopo da proteção:

1. Abra a janela **Configurações do escopo da proteção**.

2. Abra a lista suspensa na parte esquerda superior da janela e selecione **Visualização em árvore**.

3. Abra o menu de contexto da unidade virtual à qual deseja adicionar uma pasta ou arquivo e selecione uma das seguintes opções:

   - **Adicionar pasta virtual** - se desejar adicionar uma pasta virtual ao escopo da proteção.

   - **Adicionar arquivo virtual** - se desejar adicionar um arquivo virtual ao escopo da proteção.

4. No campo de entrada, especifique o nome da pasta ou arquivo.

5. Na linha que contém o nome da pasta ou arquivo criado, selecione a caixa de seleção para incluir essa pasta ou arquivo no escopo da proteção.

6. Na janela **Configurações do escopo da proteção**, clique no botão **Salvar**.

As configurações da tarefa especificadas serão salvas.

Definição manual de configurações de segurança

Por padrão, a tarefa de Proteção do Computador em Tempo Real usa as configurações de segurança comuns para todo o escopo da proteção. Estas configurações correspondem ao nível de segurança predefinido **Recomendado**.

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 itens individuais na lista de recursos de arquivos ou nós da árvore do dispositivo.

Ao trabalhar com a árvore de recursos de arquivos do dispositivo protegido, as configurações de segurança definidas para o node principal selecionado são automaticamente aplicadas a todos os nodes secundários. As configurações de segurança do node principal não são aplicadas a nós filhos configurados separadamente.

Para definir as configurações de segurança manualmente:

1. Abra a janela **Configurações do escopo da proteção**.
2. Na seção esquerda da janela, selecione o node para definir as configurações de segurança.

   Um modelo predefinido de configurações de segurança pode ser aplicado em um nó ou item selecionado no escopo da proteção.

   Na parte esquerda da janela, é possível selecionar a exibição de recursos de arquivos de rede, criar um escopo de proteção ou criar um escopo de proteção virtual.
3. Na parte direita da janela, execute uma das seguintes ações:
   - Na guia **Nível de segurança**, selecione o nível de segurança a ser aplicado.
   - Defina as configurações de segurança para o node ou item selecionado de acordo com seus requisitos:
     - **Geral**
     - **Ações**
     - **Desempenho**
4. Na janela **Configurações do escopo da proteção**, clique no botão **Salvar**.

As novas configurações de escopo da proteção são salvas.

Seleção de níveis de segurança predefinidos para a tarefa de Proteção de Arquivos em Tempo Real

É possível aplicar um dos seguintes três níveis de segurança predefinidos para um nó selecionado na árvore ou lista de recursos de arquivos do dispositivo protegido: **Desempenho máximo**, **Recomendado** e **Proteção máxima**.

Para selecionar um dos níveis de segurança predefinidos:

1. Abra a janela **Configurações do escopo da proteção**.
2. Na árvore ou na lista de recursos de arquivos de rede do dispositivo protegido, selecione um nó ou item para definir o nível de segurança predefinido.
3. Certifique-se de que o node ou item selecionado seja incluído no escopo da proteção.
4. Na parte direita da janela, na guia **Nível de segurança**, selecione o nível de segurança a ser aplicado.

   A janela exibe a lista de configurações de segurança correspondentes ao nível de segurança selecionado.
5. Clique no botão **Salvar**.

   As configurações da tarefa serão salvadas e aplicadas imediatamente à tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

Definir configurações gerais de tarefas

Para definir as configurações gerais da tarefa de Proteção de Arquivos em Tempo Real:

1. Abra a janela **Configurações do escopo da proteção**.
2. Abra a guia **Geral**.
3. Na seção **Proteção de objetos**, especifique os objetos que deseja incluir no escopo da proteção:
   - **Todos os objetos**
   - **Objetos verificados por formato**
   - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**
   - **Objetos verificados pela lista de extensões especificada**
   - **Verificar setores de inicialização do disco e MBR**
   - **Verificar fluxos NTFS alternativos**
4. No grupo **Desempenho**, marque ou desmarque a caixa de seleção **Proteger somente arquivos novos e modificados**.

   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. No bloco **Proteção de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da proteção:
   - **Todos**/**Apenas novos arquivos compactados**
   - **Todos**/**Apenas novos arquivos compactados SFX**
   - **Todos**/**Apenas novos bancos de dados de e-mail**

- **Todos** / **Apenas novos objetos compactados**
- **Todos** / **Apenas novos e-mails sem formatação**
- **Todos** / **Apenas novos objetos OLE incorporados**

6. Clique no botão **Salvar**.

A nova configuração de tarefa será salva.

Configurar ações

Para configurar ações em objetos infectados e outros objetos detectados durante a tarefa de Proteção de Arquivos em Tempo Real:

1. Abra a janela **Configurações do escopo da proteção**.
2. Selecione a guia **Ações**.
3. Selecione a ação a ser executada em objetos infectados e outros objetos detectados:
   - **Somente notificações**.
   - **Bloquear o acesso**.
   - **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**.
   - **Bloquear o acesso**.
   - **Executar ação adicional**
     Selecionar ação da lista suspensa:
     - **Quarentena**.
     - **Remover**.
     - **Recomendado**.
5. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:
   a. Desmarque ou marque a caixa **Executar ações dependendo do tipo de objeto detectado**.

b. Clique no botão **Configurações**.

c. Na janela que se abre, selecione uma ação primária e uma ação secundária (a ser executada se a ação primária falhar) para cada tipo de objeto detectado.

d. Clique no botão **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 o objeto incorporado**.

7. Clique no botão **Salvar**.

A nova configuração de tarefa será salva.

Configurar o desempenho

Para definir configurações de desempenho da tarefa de Proteção de Arquivos em Tempo Real:

1. Abra a janela **Configurações do escopo da proteção**.

2. Selecione a guia **Desempenho**.

3. No bloco **Exclusões**:

   - Desmarque ou marque a caixa de seleção **Excluir arquivos**.
   - Desmarque ou marque a caixa **Não detectar**.
   - Clique no botão **Editar** de cada configuração para adicionar exclusões.

4. No bloco **Configurações avançadas**:

   - **Parar a verificação se demorar mais que (s)**
   - **Não verificar objetos compostos com mais de (MB)**
   - **Usar a tecnologia iSwift**
   - **Usar a tecnologia iChecker**

Estatísticas da tarefa de Proteção de Arquivos em Tempo Real

Quando a tarefa de Proteção de arquivos em tempo real está sendo executada, é possível visualizar informações detalhadas em tempo real sobre o número de objetos processados pelo Kaspersky Embedded Systems Security for Windows desde que a tarefa foi iniciada.

Para exibir as estatísticas da tarefa de Proteção de Arquivos em Tempo Real:

1. Na árvore do Console do Aplicativo, expanda o node **Proteção do Computador em Tempo Real**.

2. Selecione o node secundário **Proteção de Arquivos em Tempo Real**.

As estatísticas de tarefas são exibidas na seção **Estatísticas** do painel de resultados do nó selecionado.

É possível visualizar as informações sobre os objetos processados pelo Kaspersky Embedded Systems Security for Windows desde que foi iniciado (veja a tabela abaixo).

Estatísticas da tarefa de Proteção de Arquivos em Tempo Real

Campo	Descrição
Detectado	Número total de objetos detectados pelo Kaspersky Embedded Systems Security for Windows. Por exemplo, se o Kaspersky Embedded Systems Security for Windows detectar um objeto malicioso em cinco arquivos, o valor desse campo aumentará em um.
Objetos infectados e outros detectados	O número de objetos que o Kaspersky Embedded Systems Security for Windows encontrou e classificou como infeccionado ou o número de arquivos de software legítimos encontrados que podem ser usados por invasores para danificar seu dispositivo ou dados pessoais.
Objetos possivelmente infectados detectados	Número de objetos encontrados pelo Kaspersky Embedded Systems Security for Windows que estão possivelmente infectados.
Objetos não desinfectados	Número de objetos que o Kaspersky Embedded Systems Security for Windows não desinfectou pelos seguintes motivos: • O objeto detectado é de um tipo que não pode ser desinfectado. • Ocorreu um erro durante a desinfecção.
Objetos não movidos para a Quarentena	Número de objetos que o Kaspersky Embedded Systems Security for Windows tentou colocar na Quarentena sem sucesso devido a espaço insuficiente no disco.
Objetos não removidos	Número de objetos que o Kaspersky Embedded Systems Security for Windows tentou excluir sem sucesso, devido, por exemplo, a um bloqueio no acesso ao objeto por parte de outro aplicativo.
Objetos não verificados	Número de objetos no escopo de proteção que o Kaspersky Embedded Systems Security for Windows não verificou devido, por exemplo, ao acesso ao objeto estar bloqueado por outro aplicativo.
Objetos sem backup	Número de objetos cujas cópias o Kaspersky Embedded Systems Security for Windows tentou salvar no Backup sem sucesso, devido, por exemplo, a espaço de disco insuficiente.
Erros de processamento	Número de objetos cujo processamento resultou em um erro.
Objetos desinfectados	Número de objetos desinfectados pelo Kaspersky Embedded Systems Security for Windows.
Movidos para a Quarentena	Número de objetos colocados na Quarentena pelo Kaspersky Embedded Systems Security for Windows.
Movidos para o backup	Número objetos cujas cópias o Kaspersky Embedded Systems Security for Windows salvou no Backup.
Objetos removidos	Número de objetos removidos pelo Kaspersky Embedded Systems Security for Windows.
Objetos protegidos por senha	Número de objetos (arquivos compactados, por exemplo) que o Kaspersky Embedded Systems Security for Windows ignorou porque estavam protegidos por senha.

Objetos corrompidos	Número de objetos ignorados pelo Kaspersky Embedded Systems Security for Windows porque seu formato estava corrompido.
Objetos processados	Número total de objetos processados pelo Kaspersky Embedded Systems Security for Windows.

É possível visualizar as estatísticas da tarefa de Proteção de Arquivos em Tempo Real no log de tarefas ao clicar no link **Abrir log de tarefas** na seção **Gerenciamento** no painel de detalhes.

Se o valor do campo **Total de eventos** na janela do log de tarefas de Proteção de Arquivos em Tempo Real exceder 0, recomendamos processar manualmente os eventos no log de tarefas na guia **Eventos**.

Gerenciamento da tarefa de Proteção de Arquivos em Tempo Real por meio do Plug-in da Web

Nesta seção, saiba como gerenciar a tarefa de Proteção de Arquivos em Tempo Real por meio da interface do plug-in da Web.

Configuração da tarefa de Proteção de Arquivos em Tempo Real

O nível de segurança predefinido não pode ser alterado para a tarefa de Proteção de Arquivos em Tempo Real por meio do Plug-in da Web.

Para configurar a tarefa de Proteção de Arquivos em Tempo Real por meio do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Proteção do Computador em Tempo Real**.
5. Clique em **Configurações** na subseção **Proteção de Arquivos em Tempo Real**.
6. Defina as configurações descritas na tabela a seguir.

Configurações da tarefa de Proteção de Arquivos em Tempo Real

Configuração	Descrição
Modo inteligente	O Kaspersky Embedded Systems Security for Windows seleciona objetos a serem verificados de maneira independente. Um objeto é verificado ao ser aberto e novamente depois de ser salvo, caso tenha sido modificado. Se o objeto for acessado várias vezes e modificado pelo processo, o Kaspersky Embedded Systems Security for Windows verifica o objeto novamente somente após o objeto ter sido salvo pelo processo pela última vez.
Ao acessar	O Kaspersky Embedded Systems Security for Windows verifica todos os objetos quando são abertos para a leitura, execução ou modificação.

Ao acessar e modificar	O Kaspersky Embedded Systems Security for Windows verifica um objeto quando ele é aberto e novamente após ele ser salvo, caso tenha sido modificado. Esta opção é selecionada por padrão.
Ao executar	O Kaspersky Embedded Systems Security for Windows verificará um arquivo apenas quando for acessado para execução.
Análise profunda de processos sendo inicializados (a inicialização do processo é bloqueada até que a análise termine)	O Kaspersky Embedded Systems Security for Windows realiza análises mais longas dos processos de inicialização com maior probabilidade de detectar uma ameaça. A inicialização do processo é bloqueada até o final da análise.
Usar o Analisador heurístico	Esta caixa ativa/desativa o analisador heurístico durante a verificação do objeto. Se a caixa de seleção estiver marcada, o Analisador Heurístico será ativado. Se a caixa de seleção estiver desmarcada, o Analisador Heurístico será desativado. A caixa de seleção é marcada por padrão.
Nível de análise heurística	O nível de análise heurística define o equilíbrio entre o rigor das pesquisas em busca de ameaças, a carga sobre os recursos do sistema operacional e o tempo necessário para a verificação. Estão disponíveis os seguintes níveis de sensibilidade da verificação: • **Superficial**. O analisador heurístico executa menos instruções 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 o número de instruções dos arquivos executáveis recomendado pelos especialistas da Kaspersky. Este nível é selecionado por padrão. • **Profundo**. O analisador heurístico executa mais instruções nos arquivos executáveis. De certa forma, a probabilidade de detectar ameaças nesse modo é maior. A verificação usa mais recursos do sistema, leva mais tempo e pode produzir um número mais alto de falsos positivos. A configuração estará disponível se a caixa de seleção **Usar o analisador heurístico** estiver marcada.
Aplicar Zona Confiável	Esta caixa de seleção ativa/desativa o uso da zona confiável em uma tarefa. Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows adicionará as operações de arquivos de processos confiáveis às exclusões de verificação definidas nas configurações de tarefa. Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security for Windows desconsiderará as operações de arquivo de processos confiáveis ao formar o escopo da proteção para a tarefa. A caixa de seleção é marcada por padrão.
Usar a KSN para proteção	Esta caixa ativa ou desativa o uso de serviços da KSN. Se a caixa for selecionada, o aplicativo usa dados da Kaspersky Security Network para assegurar que o aplicativo responde mais rapidamente a novas ameaças e reduza a probabilidade de falsos positivos.

	Se a caixa estiver desmarcada, a tarefa não usará serviços da KSN. A caixa de seleção é marcada por padrão.
Bloquear o acesso a recursos de rede compartilhados para sessões que exibem atividade maliciosa	A caixa de seleção ativa ou desativa o bloqueio da sessão atual e controla a disponibilidade de recursos compartilhados da rede em termos da sessão atual. Caso a caixa de seleção esteja marcada, o Kaspersky Embedded Systems Security for Windows bloqueia a sessão atual e, em termos da sessão atual, torna os recursos compartilhados de rede indisponíveis para hosts para os quais foi detectada atividade maliciosa na seção armazenamento de hosts bloqueados Caso a caixa de seleção esteja desmarcada, as condições não serão aplicadas e o Kaspersky Embedded Systems Security for Windows funcionará normalmente. Por padrão, a caixa de seleção fica desmarcada. Você pode visualizar a lista de hosts bloqueados no Armazenamento de Hosts Bloqueados. É possível restaurar o acesso aos hosts bloqueados e especificar quantos dias, horas e minutos depois do bloqueio eles poderão recuperar o acesso aos recursos de arquivos de rede pela definição das configurações de Armazenamento de Hosts Bloqueados.
Iniciar a verificação de áreas críticas quando uma infecção ativa for detectada	Se a caixa de seleção estiver marcada, quando uma infecção ativa for detectada, o Kaspersky Embedded Systems Security for Windows criará e iniciará uma tarefa temporária de Verificação de Áreas Críticas. Quando a tarefa temporária de Verificação de Áreas Críticas for concluída, o Kaspersky Embedded Systems Security for Windows a removerá. Se a caixa de seleção estiver desmarcada, quando a infecção ativa for detectada, o Kaspersky Embedded Systems Security for Windows não criará nem iniciará a tarefa de Verificação de Áreas Críticas. A caixa de seleção é marcada por padrão.
Escopo da proteção	É possível definir configurações de segurança do escopo da proteção.

Configuração do escopo de proteção da tarefa

Para configurar o escopo de proteção para a tarefa de Proteção de Arquivos em Tempo Real:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Proteção do Computador em Tempo Real**.
5. Clique em **Configurações** na subseção **Proteção de Arquivos em Tempo Real**.
6. Selecione a seção **Escopo da proteção**.
7. Execute uma das seguintes ações:

- Clique no botão **Adicionar** para adicionar uma nova regra.
- Selecione uma regra existente e clique no botão **Editar**.

A janela **Editar escopo** é aberta.

8. Mude o botão de alternância para **Ativa** e selecione um tipo de objeto.
9. Na seção **Proteção de objetos**, defina as seguintes configurações:
   - **Modo de proteção de objetos**:
     - Todos os objetos
     - Objetos verificados por formato
     - Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus
     - Objetos verificados pela lista de extensões especificada
   - Verificar setores de inicialização do disco e MBR
   - Verificar fluxos NTFS alternativos
10. Na seção **Proteção de objetos**, marque ou desmarque a caixa de seleção Proteger somente arquivos novos e modificados.
11. Na seção **Proteção de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da verificação:
    - Arquivos compactados
    - Arquivos compactados SFX
    - Objetos compactados
    - Bancos de dados de e-mail
    - E-mail sem formatação
    - Objetos OLE incorporados
    - Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado
12. Selecione a ação a ser executada em objetos infectados e outros objetos detectados:
    - Somente notificações.
    - Bloquear o acesso.
    - **Executar ação adicional**.

      Selecionar ação da lista suspensa:
      - **Desinfectar**.

- **Desinfectar. Remover se a desinfecção falhar**.
- **Remover**.
- **Recomendado**.

13. Selecione a ação a ser executada em objetos possivelmente infectados:

- **Somente notificações**.
- **Bloquear o acesso**.
- **Executar ação adicional**.

  Selecionar ação da lista suspensa:

  - **Quarentena**.
  - **Remover**.
  - **Recomendado**.

14. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:

a. Desmarque ou marque a caixa **Executar ações dependendo do tipo de objeto detectado**.

b. Clique no botão **Configurações**.

c. Na janela que se abre, selecione uma ação primária e uma ação secundária (a ser executada se a ação primária falhar) para cada tipo de objeto detectado.

d. Clique no botão **OK**.

15. Na seção **Exclusões**, é possível definir as seguintes configurações:

- Desmarque ou marque a caixa de seleção **Excluir arquivos**.
- Desmarque ou marque a caixa **Não detectar**.

16. Na seção **Desempenho**, defina as seguintes configurações:

- **Parar a verificação se demorar mais que (s)**
- **Não verificar objetos compostos com mais de (MB)**
- **Usar a tecnologia iSwift**
- **Usar a tecnologia iChecker**

17. Clique no botão **OK**.

Uso da KSN

Esta seção contém informações sobre a tarefa de Uso da KSN e como configurá-la.

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 sobre a reputação de arquivos, de recursos da web e de programas. A Kaspersky Security Network permite ao Kaspersky Embedded Systems Security for Windows 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 for Windows da Kaspersky Security Network referem-se apenas à reputação de programas.

A participação na KSN permite que a Kaspersky 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, processamento, armazenamento e destruição de informações sobre a utilização do aplicativo estão disponíveis na janela **Declaração da Kaspersky Security Network** da tarefa de utilização da KSN e na Política de Privacidade no site da Kaspersky.

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 for Windows. É possível modificar a sua decisão sobre a participação na Kaspersky Security Network a qualquer momento.

O Kaspersky Security Network pode ser usado nas seguintes tarefas do Kaspersky Embedded Systems Security for Windows:

- Proteção de Arquivos em Tempo Real.
- Verificação por Demanda.
- Regras de 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*.

Caso use a KSN Privada no dispositivo, na janela **Declaração da Kaspersky Security Network** da tarefa de Uso da KSN, é possível ler a Declaração da KSN e ativar a tarefa ao marcar a caixa de seleção **Eu aceito os termos de participação da Kaspersky 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 dispositivo, será necessário aceitar a Declaração da KSN na janela **Declaração da Kaspersky Security Network** 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 de seleção **Eu aceito os termos de participação da Kaspersky Security Network**: o aplicativo interrompe todo o processamento de dados relacionado à KSN e também 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 for Windows: todo processamento de dados relacionado à KSN é interrompido.
- Desinstalar uma chave de licença do Kaspersky Embedded Systems Security for Windows ou licença suspensa: todo o processamento de dados relacionado à KSN é interrompido.

Configurações padrão da tarefa de Uso da KSN

É possível alterar as configurações padrão da tarefa de Uso da KSN (consulte a tabela abaixo).

Configurações padrão da tarefa de Uso da KSN

Configuração	Valor padrão	Descrição
Ação a ser executada nos objetos não confiáveis da KSN	Remover	É possível especificar as ações que o Kaspersky Embedded Systems Security for Windows executará quanto a objetos identificados pela KSN como não confiáveis.
Transferência de dados	A soma de verificação de arquivo (hash MD5) é calculada para arquivos que não	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

	excedam 2 MB de tamanho.	Kaspersky Embedded Systems Security for Windows calculará o hash MD5 para arquivos de qualquer tamanho.
Programação de inicialização da 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. É possível alterar esta configuração apenas por meio do Plug-in de Administração.
Eu aceito os termos de participação da Kaspersky Security Network	Desmarcada	Caso seja selecionado, a participação na KSN após a instalação é aceita. É possível alterar a 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.

Gerenciamento do Uso da KSN por meio do Plug-in de Administração

Nesta seção, saiba como configurar a tarefa de Uso da KSN e o Gerenciamento de dados por meio do Plug-in de Administração.

Configurando a tarefa de Uso da KSN

Para configurar a tarefa de Uso da KSN:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Proteção do Computador em Tempo Real**, clique no botão **Configurações** na subseção **Uso da KSN**.

   A janela **Uso da KSN** é exibida.

5. 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 for Windows deverá executar se detectar um objeto identificado pela KSN como infectado:
     - **Remover**
     - **Registrar informações**
   - Na seção **Transferência de dados**, restrinja o tamanho dos arquivos para que a soma de verificação seja calculada:
     - Marque ou desmarque a caixa de seleção **Não calcular a soma de verificação antes de enviar para a KSN se o tamanho do arquivo ultrapassar (MB)**.
     - Se necessário, no campo à direita, altere o tamanho máximo de arquivos para os quais o Kaspersky Embedded Systems Security for Windows calcula a soma de verificação.
   - Na seção **Proxy da KSN**, desmarque ou marque a caixa de seleção **Usar o Kaspersky Security Center como Proxy da KSN**.

     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.

6. Caso necessário, configure a programação de inicialização da tarefa na guia **Gerenciamento da tarefa**. Por exemplo, você pode ativar a inicialização de tarefa por programação e especificar a frequência da inicialização da tarefa **Ao iniciar o aplicativo** se desejar que a tarefa seja executada automaticamente quando o dispositivo protegido for reiniciado.

   O aplicativo iniciará automaticamente a tarefa de Uso da KSN de acordo com a programação.

7. Configure o Manuseio de dados antes de iniciar a tarefa.

8. Clique no botão **OK**.

As configurações modificadas são aplicadas. A data e hora da modificação das configurações, bem como informações sobre as configurações de tarefa antes e depois da modificação, são salvas no log de auditoria do sistema.

Configuração do processamento de dados

Para configurar quais dados serão processados pelos serviços da KSN e aceitar a Declaração da KSN:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Proteção do Computador em Tempo Real** clique no botão **Declaração da KSN** na subseção **Uso da KSN**.

   A janela **Declaração da Kaspersky Security Network** é exibida.

5. Na guia **Estatísticas e serviços**, leia a Declaração e marque a caixa de seleção **Eu aceito os termos de participação da Kaspersky Security Network**.

6. Para aumentar o nível de proteção, as seguintes caixas são selecionadas automaticamente:

   - **Enviar dados dos arquivos verificados**

   - **Enviar as estatísticas da Kaspersky Security Network**

   Você pode desmarcar estas caixas e deixar de enviar dados adicionais a qualquer momento.

7. A caixa de seleção **Enviar as estatísticas da Kaspersky Security Network** é selecionada por padrão. É possível desmarcar a caixa de seleção a qualquer momento caso não queira que o Kaspersky Embedded Systems Security for Windows envie estatísticas adicionais para a Kaspersky.

8. Clique no botão **OK**.

   A configuração de processamento de dados será salva.

Gerenciamento do Uso da KSN por meio do Console do Aplicativo

Nesta seção, aprenda como configurar a tarefa de Uso da KSN e Manuseio de dados por meio do Console do Aplicativo.

Configurando a tarefa de Uso da KSN

Para configurar a tarefa de Uso da KSN:

1. Na árvore do Console do Aplicativo, expanda o node **Proteção do Computador em Tempo Real**.

2. Selecione o node secundário **Uso da KSN**.

3. Clique no link **Propriedades** no painel de resultados.

   A janela **Configurações de tarefa** é exibida na guia **Geral**.

4. Configure a tarefa:

   - Na seção **Ação a ser executada nos objetos não confiáveis da KSN**, especifique a ação que o Kaspersky Embedded Systems Security for Windows deverá executar se detectar um objeto identificado pela KSN

como infectado:

- **Remover**
- **Registrar informações**

- Na seção **Transferência de dados**, restrinja o tamanho dos arquivos para que a soma de verificação seja calculada:
  - Marque ou desmarque a caixa de seleção **Não calcular a soma de verificação antes de enviar para a KSN se o tamanho do arquivo ultrapassar (MB)**.
  - Se necessário, no campo à direita, altere o tamanho máximo de arquivos para os quais o Kaspersky Embedded Systems Security for Windows calcula a soma de verificação.

5. Se necessário, configure a programação de inicialização da tarefa nas guias **Agendamento** e **Avançado**. Por exemplo, você pode ativar a inicialização de tarefa por programação e especificar a frequência da inicialização da tarefa **Ao iniciar o aplicativo** se desejar que a tarefa seja executada automaticamente quando o dispositivo protegido for reiniciado.

   O aplicativo iniciará automaticamente a tarefa de Uso da KSN de acordo com a programação.

6. Configure o Manuseio de dados antes de iniciar a tarefa.

7. Clique no botão **OK**.

As configurações modificadas são aplicadas. A data e hora da modificação das configurações, bem como informações sobre as configurações de tarefa antes e depois da modificação, são salvas no log de auditoria do sistema.

Configuração do processamento de dados

Para configurar quais dados serão processados pelos serviços da KSN e aceitar a Declaração da KSN:

1. Na árvore do Console do Aplicativo, expanda o node **Proteção do Computador em Tempo Real**.

2. Selecione o node secundário **Uso da KSN**.

3. Clique no link **Declaração da KSN** no painel de detalhes.

   A janela **Declaração da Kaspersky Security Network** é exibida.

4. Na guia **Estatísticas e serviços**, leia a Declaração e marque a caixa de seleção **Eu aceito os termos de participação da Kaspersky Security Network**.

5. Para aumentar o nível de proteção, as seguintes caixas são selecionadas automaticamente:

   - **Enviar dados dos arquivos verificados**
   - **Enviar as estatísticas da Kaspersky Security Network**

   Você pode desmarcar estas caixas e deixar de enviar dados adicionais a qualquer momento.

6. A caixa de seleção **Enviar as estatísticas da Kaspersky Security Network** é selecionada por padrão. É possível desmarcar a caixa de seleção a qualquer momento caso não queira que o Kaspersky Embedded

Systems Security for Windows envie estatísticas adicionais para a Kaspersky.

7. Clique no botão **OK**.

A configuração de processamento de dados será salva.

Gerenciamento do Uso da KSN por meio do Plug-in da Web

Para configurar a tarefa de Uso da KSN e o Tratamento de Dados por meio do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Proteção do Computador em Tempo Real**.
5. Clique em **Configurações** na subseção **Uso da KSN**.
6. Defina as configurações descritas na tabela a seguir.

Configurações da tarefa de Uso da KSN e o Tratamento de Dados por meio do Plug-in de Administração

Configuração	Descrição
Remover	O Kaspersky Embedded Systems Security for Windows exclui o objeto com o status não confiável da KSN e coloca uma cópia dele no Backup. Esta opção é selecionada por padrão.
Registrar informações em log	O Kaspersky Embedded Systems Security for Windows registra informações sobre o objeto com o status não confiável da KSN no log de tarefas. O Kaspersky Embedded Systems Security for Windows não exclui o objeto não confiável.
Não calcular a soma de verificação antes de enviar à KSN se o tamanho do arquivo exceder	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 de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows 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 for Windows calculará a soma de verificação para arquivos de qualquer tamanho. A caixa de seleção é marcada por padrão.
Confirmo que li, entendi e aceitei completamente os termos de participação na Kaspersky Security Network	Ao marcar esta caixa de seleção, você confirma que leu e aceitou os termos da Declaração da Kaspersky Security Network.
Enviar dados	

dos arquivos verificados	Se a caixa for selecionada, o Kaspersky Embedded Systems Security for Windows envia a soma de verificação dos arquivos verificados para a Kaspersky. 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 for Windows 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 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, e não podem ser configurados pelo usuário em um dispositivo 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 para proteger os servidores da KSN contra DDoS* é exibido na estatística da tarefa de Uso da KSN. A caixa de seleção é marcada por padrão.
Concorde para processar os dados como parte das estatísticas da Kaspersky Security Network	Se a caixa for selecionada o Kaspersky Embedded Systems Security for Windows 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 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 for Windows não enviará estatísticas adicionais. A caixa de seleção é marcada por padrão.
Gerenciamento de tarefas	É possível definir configurações para a inicialização programada da tarefa.

Configuração da transferência de dados adicionais

O Kaspersky Embedded Systems Security for Windows pode ser configurado para enviar os seguintes dados à Kaspersky:

- 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.

As caixas de seleção correspondentes podem ser marcadas ou desmarcadas apenas se a caixa de seleção **Eu aceito os termos de participação da Kaspersky Security Network** estiver marcada.

Por padrão, o Kaspersky Embedded Systems Security for Windows envia somas de verificação de arquivos e estatísticas adicionais após aceitar a Declaração da KSN.

A caixa de seleção **Eu aceito os termos de participação da Kaspersky Security Network** só não é editável se a política do Kaspersky Security Center bloquear alterações nas configurações do tratamento de dados.

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	Condições de estado da caixa Eu aceito os termos de participação da Kaspersky Security Network
☑	• solicitações de reputação são enviadas • a caixa pode ser editada	• estatísticas adicionais são enviadas • a caixa pode ser editada	• os termos da Declaração da Kaspersky Security Network são aceitos • a caixa pode ser editada
☑	• solicitações de reputação são enviadas • a caixa não pode ser editada	• estatísticas adicionais são enviadas • a caixa não pode ser editada	• os termos da Declaração da Kaspersky Security Network são aceitos • 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	• os termos da Declaração da Kaspersky Security Network não são aceitos • a caixa pode ser editada
☐	• solicitações de reputação não são enviadas • a caixa não pode ser editada	• estatísticas adicionais não são enviadas • a caixa não pode ser editada	• os termos da Declaração da Kaspersky Security Network não são aceitos • a caixa não pode ser editada

Estatísticas da tarefa de Uso da KSN

Enquanto uma tarefa de Uso da KSN está sendo executada, é possível visualizar informações detalhadas sobre o número de objetos processados pelo Kaspersky Embedded Systems Security for Windows desde de foi iniciado até o momento atual. As informações sobre todos os eventos que ocorrem durante a execução da tarefa são registradas no log de tarefas.

Para exibir as estatísticas da tarefa de Uso da KSN:

1. Na árvore do Console do Aplicativo, expanda o node **Proteção do Computador em Tempo Real**.
2. Selecione o node secundário **Uso da KSN**.

As estatísticas de tarefa são exibidas na seção **Estatísticas** do painel de detalhes do nó selecionado.

É possível visualizar as informações sobre os objetos processados pelo Kaspersky Embedded Systems Security for Windows desde quando a tarefa foi iniciada (consulte a tabela abaixo).

Campo	Descrição
Erros no envio de solicitações	Número de solicitações da KSN cujo processamento resultou em um erro de tarefa.
Estatísticas formadas	Número de pacotes estatísticos gerados e enviados à KSN.
Objetos removidos	Número de objetos que o Kaspersky Embedded Systems Security for Windows excluiu ao executar a tarefa de Uso da KSN.
Movidos para o backup	Número objetos cujas cópias o Kaspersky Embedded Systems Security for Windows salvou no Backup.
Objetos não removidos	O número de objetos que o Kaspersky Embedded Systems Security for Windows tentou excluir mas não conseguiu, devido, por exemplo, a um bloqueio no acesso ao objeto por parte de outro aplicativo. As informações sobre tais objetos são registradas no log de tarefas.
Objetos sem backup	O número de objetos cujas cópias o Kaspersky Embedded Systems Security for Windows tentou salvar no Backup mas não conseguiu, por exemplo, devido a espaço de disco insuficiente. O aplicativo não desinfecta ou exclui arquivos que não podem ser movidos para o Backup. As informações sobre tais objetos são registradas no log de tarefas.
Modo limitado	O status indica se o aplicativo envia solicitações de reputação de arquivo em um modo limitado. Em um modo limitado, o Kaspersky Embedded Systems Security for Windows envia apenas uma parte das solicitações de reputação do arquivo, de acordo com a recomendação dos especialistas da Kaspersky.

Proteção Contra Ameaças à Rede

Esta seção contém informações sobre a tarefa de Proteção Contra Ameaças à Rede e como configurá-la.

Sobre a tarefa de Proteção Contra Ameaças à Rede

A Proteção Contra Ameaças à Rede pode ser instalada somente em um dispositivo com o Microsoft Windows 7 e versões posteriores ou o Windows Server 2008 R2 e versões posteriores.

A tarefa de Proteção Contra Ameaças à Rede verifica o tráfego de rede de entrada em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede direcionada ao computador, o Kaspersky Embedded Systems Security for Windows bloqueará a atividade de rede do computador invasor. A tela exibirá um aviso que informa uma tentativa de ataque à rede e mostrará informações sobre o computador invasor.

Por padrão, a tarefa de Proteção Contra Ameaças à Rede é executada no modo **Bloquear conexões quando um ataque for detectado**. Nesse modo, o Kaspersky Embedded Systems Security for Windows adiciona endereços IP de hosts que mostram atividades típicas de ataques à rede na lista de hosts bloqueados.

Você pode visualizar a lista de hosts bloqueados no Armazenamento de Hosts Bloqueados.

É possível restaurar o acesso aos hosts bloqueados e especificar quantos dias, horas e minutos depois do bloqueio eles poderão recuperar o acesso aos recursos de arquivos de rede pela definição das configurações de Armazenamento de Hosts Bloqueados.

Os endereços IP de hosts que mostram atividades típicas de ataques à rede são excluídos da lista de hosts bloqueados nos seguintes casos:

- O Kaspersky Embedded Systems Security for Windows está desinstalado.
- O endereço IP foi excluído manualmente da lista de hosts bloqueados.
- O prazo de bloqueio do host expirou.
- A tarefa de Proteção Contra Ameaças à Rede foi interrompida e a caixa de seleção **Não interromper a análise de tráfego quando a tarefa não estiver em execução** está desmarcada.
- O modo **Bloquear conexões quando um ataque for detectado** foi desativado.

Configurações padrão da tarefa de Proteção Contra Ameaças à Rede

A tarefa de Proteção Contra Ameaças à Rede usa as configurações padrão descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Configurações padrão da tarefa de Proteção Contra Ameaças à Rede

Configuração	Valor padrão	Descrição
Modo de processamento	**Bloquear conexões quando um ataque for detectado**	A tarefa de Proteção Contra Ameaças à Rede pode ser iniciada no modo **Passagem**, **Informar somente sobre ataques à rede** ou **Bloquear conexões quando um ataque for detectado**.

		A caixa de seleção ativa ou desativa a adição de hosts que exibam uma atividade típica de ataques à rede na lista de hosts bloqueados. Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, registrará os eventos sobre a atividade detectada e adicionará os endereços IP de hosts que exibem atividades típicas de ataques à rede na lista de hosts bloqueados. Você pode visualizar a lista de hosts bloqueados no Armazenamento de Hosts Bloqueados. É possível restaurar o acesso aos hosts bloqueados e especificar quantos dias, horas e minutos depois do bloqueio eles poderão recuperar o acesso aos recursos de arquivos de rede pela definição das configurações de Armazenamento de Hosts Bloqueados. O modo é selecionado por padrão. Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, registrará os eventos sobre a atividade detectada, mas não bloqueará a atividade de rede no computador invasor. Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, mas não registrará os eventos sobre a atividade detectada e não bloqueará a atividade de rede no computador invasor. Por exemplo, você pode usar esse modo em caso de diminuição no desempenho do dispositivo protegido.
Exclusões	A lista de exclusão não é aplicada.	Especifique áreas que deseja excluir do escopo da proteção da tarefa.
Configurações de agendamento	Por padrão, a tarefa de Proteção contra ameaças à rede é iniciada automaticamente quando o Kaspersky Embedded Systems Security for Windows é iniciado.	É possível configurar a programação.

Configuração da tarefa de Proteção Contra Ameaças à Rede por meio do Console do Aplicativo

Nesta seção, saiba como gerenciar a tarefa de Proteção Contra Ameaças à Rede por meio da interface do Console do Aplicativo.

Configurações gerais da tarefa

Para definir as configurações gerais da tarefa de Proteção Contra Ameaças à Rede pelo Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó secundário da **Proteção Contra Ameaças à Rede**.
3. Clique no link **Proteção Contra Ameaças à Rede** no painel de detalhes do nó **Propriedades**.

   A janela **Configurações de tarefa** é aberta.
4. Abra a guia **Geral**.
5. Na seção **Modo de processamento**, selecione o modo da tarefa:

   - Passagem.

     Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, mas não registrará os eventos sobre a atividade detectada e não bloqueará a atividade de rede no computador invasor.

     Por exemplo, você pode usar esse modo em caso de diminuição no desempenho do dispositivo protegido.

   - Informar somente sobre ataques à rede.

     Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, registrará os eventos sobre a atividade detectada, mas não bloqueará a atividade de rede no computador invasor.

   - Bloquear conexões quando um ataque for detectado.

A caixa de seleção ativa ou desativa a adição de hosts que exibam uma atividade típica de ataques à rede na lista de hosts bloqueados.

Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, registrará os eventos sobre a atividade detectada e adicionará os endereços IP de hosts que exibem atividades típicas de ataques à rede na lista de hosts bloqueados.

Você pode visualizar a lista de hosts bloqueados no Armazenamento de Hosts Bloqueados.

É possível restaurar o acesso aos hosts bloqueados e especificar quantos dias, horas e minutos depois do bloqueio eles poderão recuperar o acesso aos recursos de arquivos de rede pela definição das configurações de Armazenamento de Hosts Bloqueados.

O modo é selecionado por padrão.

6. No bloco **Proteção contra MAC spoofing**, marque ou desmarque a caixa de seleção **Ativar a proteção contra os ataques de MAC spoofing**.

   Um ataque de spoofing do endereço MAC consiste em alterar o endereço MAC de um dispositivo de rede (placa de rede). Consequentemente, um invasor pode redirecionar os dados enviados de um dispositivo para outro e obter acesso a esses dados.

   Caso a caixa de seleção esteja marcada e o modo de tarefa Proteção Contra Ameaças à Rede seja diferente de **Passagem**, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de ações típicas de ataques de spoofing do endereço MAC e executará as ações de acordo com o modo de tarefa selecionado para a tarefa Proteção Contra Ameaças à Rede.

   Caso a caixa de seleção esteja desmarcada ou o modo de tarefa **Passagem** esteja selecionado, o Kaspersky Embedded Systems Security for Windows não verificará o tráfego de rede de entrada em busca de ações típicas de ataques de spoofing do endereço MAC.

   Por padrão, a caixa de seleção fica desmarcada.

7. Marque ou desmarque a caixa de seleção **Não interromper a análise de tráfego quando a tarefa não estiver em execução**.

   Caso esta caixa de controle esteja selecionada, então, mesmo quando a tarefa de Proteção Contra Ameaças à Rede for interrompida, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede e bloqueará a atividade de rede no computador invasor, dependendo do modo de tarefa selecionado.

   Caso a caixa de seleção esteja desmarcada, quando a tarefa de Proteção Contra Ameaças à Rede for interrompida, o Kaspersky Embedded Systems Security for Windows não verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede.

   Por padrão, a caixa de seleção fica desmarcada.

8. Clique no botão **OK**.

Adição de exclusões

Para adicionar as exclusões para a tarefa de Proteção contra ameaças à rede, siga as etapas a seguir:

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó secundário da **Proteção Contra Ameaças à Rede**.

3. Clique no link **Proteção Contra Ameaças à Rede** no painel de detalhes do nó **Propriedades**.

   A janela **Configurações de tarefa** é aberta.

4. Na guia **Exclusões**, marque a caixa de seleção **Não controlar endereços IP excluídos**.

   Se esta caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows não verificará o tráfego da rede de entrada em busca de endereços IP excluídos.

   Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows não aplicará a lista de exclusão.

5. Especifique o endereço IP e clique no botão **Adicionar**.

6. Clique no botão **OK**.

Configuração da tarefa de Proteção Contra Ameaças à Rede por meio do Plug-in de Administração

Nesta seção, saiba como gerenciar a tarefa de Proteção Contra Ameaças à Rede com a interface do Plug-in de Administração.

Configurações gerais da tarefa

Para configurar a tarefa de Proteção Contra Ameaças à Rede pelo Plug-in de Administração:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Proteção do Computador em Tempo Real**, no bloco **Proteção Contra Ameaças à Rede**, clique no botão **Configurações**.

   A janela **Proteção Contra Ameaças à Rede** é exibida.

5. Abra a guia **Geral**.

6. Selecione o modo de tarefa na seção **Modo de processamento**:

   - **Passagem**.

Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, mas não registrará os eventos sobre a atividade detectada e não bloqueará a atividade de rede no computador invasor.

Por exemplo, você pode usar esse modo em caso de diminuição no desempenho do dispositivo protegido.

- **Informar somente sobre ataques à rede**.

  Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, registrará os eventos sobre a atividade detectada, mas não bloqueará a atividade de rede no computador invasor.

- **Bloquear conexões quando um ataque for detectado**.

  A caixa de seleção ativa ou desativa a adição de hosts que exibam uma atividade típica de ataques à rede na lista de hosts bloqueados.

  Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, registrará os eventos sobre a atividade detectada e adicionará os endereços IP de hosts que exibem atividades típicas de ataques à rede na lista de hosts bloqueados.

  Você pode visualizar a lista de hosts bloqueados no Armazenamento de Hosts Bloqueados.

  É possível restaurar o acesso aos hosts bloqueados e especificar quantos dias, horas e minutos depois do bloqueio eles poderão recuperar o acesso aos recursos de arquivos de rede pela definição das configurações de Armazenamento de Hosts Bloqueados.

  O modo é selecionado por padrão.

7. No bloco **Proteção contra MAC spoofing**, marque ou desmarque a caixa de seleção **Ativar a proteção contra os ataques de MAC spoofing**.

   Um ataque de spoofing do endereço MAC consiste em alterar o endereço MAC de um dispositivo de rede (placa de rede). Consequentemente, um invasor pode redirecionar os dados enviados de um dispositivo para outro e obter acesso a esses dados.

   Caso a caixa de seleção esteja marcada e o modo de tarefa Proteção Contra Ameaças à Rede seja diferente de **Passagem**, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de ações típicas de ataques de spoofing do endereço MAC e executará as ações de acordo com o modo de tarefa selecionado para a tarefa Proteção Contra Ameaças à Rede.

   Caso a caixa de seleção esteja desmarcada ou o modo de tarefa **Passagem** esteja selecionado, o Kaspersky Embedded Systems Security for Windows não verificará o tráfego de rede de entrada em busca de ações típicas de ataques de spoofing do endereço MAC.

   Por padrão, a caixa de seleção fica desmarcada.

8. Marque ou desmarque a caixa de seleção **Não interromper a análise de tráfego quando a tarefa não estiver em execução**.

Caso esta caixa de controle esteja selecionada, então, mesmo quando a tarefa de Proteção Contra Ameaças à Rede for interrompida, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede e bloqueará a atividade de rede no computador invasor, dependendo do modo de tarefa selecionado.

Caso a caixa de seleção esteja desmarcada, quando a tarefa de Proteção Contra Ameaças à Rede for interrompida, o Kaspersky Embedded Systems Security for Windows não verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede.

Por padrão, a caixa de seleção fica desmarcada.

9. Clique no botão **OK**.

Adição de exclusões

Para adicionar as exclusões para a tarefa de Proteção contra ameaças à rede, siga as etapas a seguir:

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Proteção do Computador em Tempo Real**, clique no botão **Configurações** na subseção **Proteção Contra Ameaças à Rede**.

   A janela **Proteção Contra Ameaças à Rede** é exibida.
5. Na guia **Exclusões**, marque a caixa de seleção **Não controlar endereços IP excluídos**.

   Se esta caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows não verificará o tráfego da rede de entrada em busca de endereços IP excluídos.

   Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows não aplicará a lista de exclusão.
6. Especifique o endereço IP e clique no botão **Adicionar**.
7. Clique no botão **OK**.

Configuração da tarefa de Proteção Contra Ameaças à Rede por meio do Plug-in da Web

Nesta seção, saiba como gerenciar a tarefa de Proteção Contra Ameaças à Rede por meio da interface do Plug-in da Web.

Configurações gerais da tarefa

Para definir as configurações gerais da tarefa Proteção Contra Ameaças à Rede com o uso do Web Console:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Proteção do Computador em Tempo Real**.
5. No bloco **Proteção Contra Ameaças à Rede**, clique no botão **Configurações**.

   A janela **Proteção Contra Ameaças à Rede** é exibida.
6. Selecione a guia **Geral**.
7. Na seção **Modo de processamento**, selecione o modo de processamento:

   - **Passagem**.

     Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, mas não registrará os eventos sobre a atividade detectada e não bloqueará a atividade de rede no computador invasor.

     Por exemplo, você pode usar esse modo em caso de diminuição no desempenho do dispositivo protegido.

   - **Informar somente sobre ataques à rede**.

     Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, registrará os eventos sobre a atividade detectada, mas não bloqueará a atividade de rede no computador invasor.

   - **Bloquear conexões quando um ataque for detectado**.

     A caixa de seleção ativa ou desativa a adição de hosts que exibam uma atividade típica de ataques à rede na lista de hosts bloqueados.

     Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede, registrará os eventos sobre a atividade detectada e adicionará os endereços IP de hosts que exibem atividades típicas de ataques à rede na lista de hosts bloqueados.

     Você pode visualizar a lista de hosts bloqueados no Armazenamento de Hosts Bloqueados.

     É possível restaurar o acesso aos hosts bloqueados e especificar quantos dias, horas e minutos depois do bloqueio eles poderão recuperar o acesso aos recursos de arquivos de rede pela definição das configurações de Armazenamento de Hosts Bloqueados.

     O modo é selecionado por padrão.
8. No bloco **Proteção contra MAC spoofing**, marque ou desmarque a caixa de seleção **Ativar a proteção contra os ataques de MAC spoofing**.

Um ataque de spoofing do endereço MAC consiste em alterar o endereço MAC de um dispositivo de rede (placa de rede). Consequentemente, um invasor pode redirecionar os dados enviados de um dispositivo para outro e obter acesso a esses dados.

Caso a caixa de seleção esteja marcada e o modo de tarefa Proteção Contra Ameaças à Rede seja diferente de **Passagem**, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de ações típicas de ataques de spoofing do endereço MAC e executará as ações de acordo com o modo de tarefa selecionado para a tarefa Proteção Contra Ameaças à Rede.

Caso a caixa de seleção esteja desmarcada ou o modo de tarefa **Passagem** esteja selecionado, o Kaspersky Embedded Systems Security for Windows não verificará o tráfego de rede de entrada em busca de ações típicas de ataques de spoofing do endereço MAC.

Por padrão, a caixa de seleção fica desmarcada.

9. Marque ou desmarque a caixa de seleção **Não interromper a análise de tráfego quando a tarefa não estiver em execução**.

Caso esta caixa de controle esteja selecionada, então, mesmo quando a tarefa de Proteção Contra Ameaças à Rede for interrompida, o Kaspersky Embedded Systems Security for Windows verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede e bloqueará a atividade de rede no computador invasor, dependendo do modo de tarefa selecionado.

Caso a caixa de seleção esteja desmarcada, quando a tarefa de Proteção Contra Ameaças à Rede for interrompida, o Kaspersky Embedded Systems Security for Windows não verificará o tráfego de rede de entrada em busca de atividades típicas de ataques à rede.

Por padrão, a caixa de seleção fica desmarcada.

10. Clique no botão **OK**.

Adição de exclusões

Para adicionar as exclusões para a tarefa de Proteção contra ameaças à rede, siga as etapas a seguir:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos → Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Proteção do Computador em Tempo Real**.
5. Clique no botão **Configurações** na subseção **Proteção Contra Ameaças à Rede**.
6. Na guia **Exclusões**, marque a caixa de seleção **Não controlar endereços IP excluídos**.

Se esta caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows não verificará o tráfego da rede de entrada em busca de endereços IP excluídos.

Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows não aplicará a lista de exclusão.

7. Especifique o endereço IP e clique no botão **Adicionar**.

8. Clique no botão **OK**.

Controle de Inicialização de Aplicativos

Esta seção contém informações sobre a tarefa de Controle de Inicialização de Aplicativos e como configurá-la.

Sobre a tarefa de Controle de Inicialização de Aplicativos

Durante a execução da tarefa de Controle de Inicialização de Aplicativos, o Kaspersky Embedded Systems Security for Windows monitora as tentativas de inicialização de aplicativos por usuários e permite ou nega a inicialização desses aplicativos. A tarefa de Controle de Inicialização de Aplicativos baseia-se no princípio de Negação Padrão, o que significa que qualquer aplicativo que não tenha permissão configurada na tarefa será automaticamente bloqueado.

Você pode permitir a inicialização de aplicativos usando um dos seguintes métodos:

- Definir regras de permissão para aplicativos confiáveis.
- Verificar a reputação de aplicativos confiáveis na KSN na inicialização.

A tarefa dá a prioridade máxima à negação da inicialização de aplicativos. Por exemplo, se um aplicativo for impedido de iniciar por uma das regras de bloqueio, a inicialização do aplicativo será negada independentemente da conclusão confiável da KSN. Nesse caso, se o aplicativo for considerado não confiável pelos serviços da KSN, mas estiver incluído no escopo de uma regra de permissão, sua inicialização será negada.

Todas as tentativas de iniciar aplicativos são registradas no log de tarefas.

A tarefa de Controle de Inicialização de Aplicativos pode operar em um de dois modos:

- **Ativa**. O Kaspersky Embedded Systems Security for Windows usa um conjunto de regras para controlar a inicialização de aplicativos que se enquadram no escopo das regras de Controle de Inicialização de Aplicativos. O escopo das regras de Controle de Inicialização de Aplicativos é especificado nas configurações dessa tarefa. Se um aplicativo se enquadrar no escopo das regras de Controle de Inicialização de Aplicativos, e as configurações da tarefa não satisfizerem alguma regra especificada, a inicialização do aplicativo será negada.

  A inicialização dos aplicativos que não se enquadram no escopo de nenhuma regra especificada nas configurações da tarefa de Controle de Inicialização de Aplicativos é bloqueada, independentemente das configurações da tarefa de Controle de Inicialização de Aplicativos.

  A tarefa de **Controle de Inicialização de Aplicativos** não pode ser iniciada no modo Ativa se nenhuma regra tiver sido criada ou se houver mais de 65.535 regras para um dispositivo protegido.

- **Somente estatísticas**. O Kaspersky Embedded Systems Security for Windows não usa as regras de Controle de Inicialização de Aplicativos para permitir ou negar a inicialização de aplicativos. Em vez disso, ele apenas registra informações sobre a inicialização de aplicativos, sobre as regras atendidas pelos aplicativos em execução e ações que seriam executadas se a tarefa estivesse sendo executada no modo **Ativa**. Todos os aplicativos podem ser inicializados. Este modo está definido por padrão.

  Você pode usar esse modo para criar regras de Controle de Inicialização de Aplicativos com base nas informações registradas no log de tarefas.

Você pode configurar a tarefa de Controle de Inicialização de Aplicativos de acordo com um dos seguintes cenários:

- Configuração avançada e aplicação de regras de controle de inicialização de aplicativos.
- Configuração básica de regra e Uso da KSN para o Controle de Inicialização de Aplicativos.

Se os arquivos do sistema operacional estiverem enquadrados no escopo da tarefa de Controle de Inicialização de Aplicativos, recomendamos que, ao criar as regras de Controle de Inicialização de Aplicativos, você se certifique de tais aplicativos devem ser permitidos pela criação de novas regras. Caso contrário, o sistema operacional pode não conseguir ser iniciado.

O Kaspersky Embedded Systems Security for Windows também intercepta processos iniciados sob o Subsistema do Windows para Linux (exceto scripts executados no shell do UNIX™ ou interpretadores da linha de comando). Para tais processos, a tarefa de Controle de Inicialização de Aplicativos aplica a ação definida pela configuração atual. A tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos reconhece a inicialização do aplicativo e gera regras correspondentes para aplicativos executados sob o Subsistema do Windows para Linux.

Sobre as regras do Controle de Inicialização de Aplicativos

Como funcionam as regras de Controle de Inicialização de Aplicativos

A operação das regras de Controle de Inicialização de Aplicativos é baseada nos seguintes componentes:

- Tipo de regra.

  As regras de Controle de Inicialização de Aplicativos podem permitir ou negar a inicialização de um aplicativo. Consequentemente, elas são chamadas de regras de *permissão* ou *negação*. Para criar uma lista de regras de permissão para o Controle de Inicialização de Aplicativos, você pode usar o Gerador de Regras para gerar regras de permissão ou usar a tarefa de Controle de Inicialização de Aplicativos no modo **Somente estatísticas**. Você também pode adicionar regras de permissão manualmente.

- Usuário ou grupo de usuários.

  As regras de Controle de Inicialização de Aplicativos podem controlar a inicialização de aplicativos específicos por um usuário e/ou grupo de usuários.

- Escopo de uso da regra.

  As regras de Controle de Inicialização de Aplicativos podem ser aplicadas à inicialização de *arquivos executáveis*, *scripts* e *pacotes MSI*.

- Critério para acionamento de regras.

  As regras de Controle de Inicialização de Aplicativos controlam a inicialização de arquivos que satisfazem a um dos critérios especificados nas configurações da regra: assinado pelo *certificado digital* especificado, correspondente ao *hash SHA256*, localizado no *caminho* e correspondente aos argumentos especificados na *linha de comando*. É preciso selecionar ao menos uma opção. Caso contrário, a regra de Controle de Inicialização de Aplicativos não será adicionada.

  Caso o **Certificado digital** seja estabelecido como critério para acionamento de regras, a regra criada controla a inicialização de todos os aplicativos confiáveis no sistema operacional. Você pode estabelecer condições mais estritas para este critério selecionando as caixas de seleção a seguir:

  - **Usar assunto**
  - **Usar miniatura**

O uso de impressões digitais permite o acionamento mais restrito das regras de inicialização de aplicativos com base em um certificado digital, pois uma impressão digital é um identificador único de um certificado digital e não pode ser forjada, diferentemente do requerente de um certificado digital.

Você pode especificar exclusões das regras de Controle de Inicialização de Aplicativos. As exclusões das regras de Controle de Inicialização de Aplicativos são baseadas nos mesmos critérios usados para acionar as regras: certificado digital, hash SHA256 e caminho do arquivo. As exclusões das regras de Controle de Inicialização de Aplicativos podem ser necessárias para especificar certas regras de permissão: por exemplo, se você quiser permitir que os usuários iniciem aplicativos no caminho C:\Windows, enquanto bloqueia a inicialização do arquivo Regedit.exe.

Se os arquivos do sistema operacional estiverem enquadrados no escopo da tarefa de Controle de Inicialização de Aplicativos, recomendamos que, ao criar as regras de Controle de Inicialização de Aplicativos, você se certifique de tais aplicativos devem ser permitidos pela criação de novas regras. Caso contrário, o sistema operacional pode não conseguir ser iniciado.

Gerenciando regras de Controle de Inicialização de Aplicativos

Você pode executar as seguintes ações com as regras de Controle de Inicialização de Aplicativos:

- Adicionar regras manualmente.
- Gerar e adicionar regras automaticamente.
- Remover regras.
- Exportar regras para o arquivo.
- Verificar arquivos selecionados para regras que permitam a execução desses arquivos.
- Filtrar as regras na lista segundo o critério especificado.

Sobre o Controle de Distribuição de Software

Gerar regras de Controle de Inicialização de Aplicativos pode ser complicado se você também tiver que controlar a distribuição de software em um dispositivo protegido, por exemplo, em dispositivos protegidos onde o software instalado é atualizado automaticamente de maneira periódica. Nesse caso, a lista de regras de permissão deve ser atualizada 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 Distribuição de Software.

Um *pacote de distribuição de software* (doravante referido como "pacote") representa um aplicativo de software a ser instalado em um dispositivo protegido. Cada pacote contém pelo menos um aplicativo e também pode conter arquivos individuais, atualizações, ou até mesmo 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 um pacote de instalação é adicionado na lista, ele se torna confiável. A descompactação é permitida para pacotes confiáveis, e a inicialização automática é permitida para os aplicativos instalados ou atualizados a partir de pacotes confiáveis. Os arquivos extraídos podem herdar o atributo de confiabilidade do pacote primário de distribuição. Um *pacote primário de distribuição* é um pacote que foi adicionado à lista de exclusões de Controle de Distribuição de Software por um usuário e se tornou um pacote confiável.

O Kaspersky Embedded Systems Security for Windows 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 desativado ou o componente de 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** estiver desmarcada nas configurações da tarefa de Controle de Inicialização de Aplicativos.

Cache de distribuição de software

O Kaspersky Embedded Systems Security for Windows usa um cache de distribuição de software gerado dinamicamente ("cache de distribuição") para estabelecer a relação entre pacotes confiáveis e arquivos criados durante a distribuição de software. Quando o pacote é iniciado pela primeira vez, o Kaspersky Embedded Systems Security for Windows detecta todos os arquivos criados pelo pacote durante o processo de distribuição de software e armazena as somas de verificação dos arquivos e os caminhos no cache de distribuição. Então todos os arquivos no cache de distribuição podem ser inicializados por padrão.

Você não pode analisar, limpar ou modificar manualmente o cache de distribuição por meio da interface de usuário. O cache é preenchido e controlado pelo Kaspersky Embedded Systems Security for Windows.

Você pode exportar o cache de distribuição para um arquivo de configuração (no formato XML) e limpar o cache usando opções de linha de comando.

Para exportar o cache de distribuição para um arquivo de configuração, execute o seguinte comando:

```
kavshell appcontrol /config /savetofile:<caminho completo> /sdc
```

Para limpar o cache de distribuição, execute o seguinte comando:

```
kavshell appcontrol /config /clearsdc
```

O Kaspersky Embedded Systems Security for Windows atualiza o cache de distribuição a cada 24 horas. Se a soma de verificação de um arquivo permitido anteriormente forem alterados, o aplicativo exclui o registro desse arquivo do cache de distribuição. Se a tarefa de Controle de Inicialização de Aplicativos for iniciada no modo Ativa, tentativas subsequentes de inicialização desse arquivo serão bloqueadas. Se o caminho completo do arquivo anteriormente permitido for alterado, as tentativas subsequentes de iniciar esse arquivo não serão bloqueadas, porque a soma de verificação é armazenada dentro do cache de distribuição.

Processamento dos arquivos extraídos

Todos os arquivos extraídos de um pacote confiável herdam o atributo de confiabilidade na primeira execução do pacote. Se você desmarcar a caixa de seleção após a primeira inicialização, todos os arquivos extraídos do pacote reterão o atributo herdado. Para reinicializar o atributo herdado em todos os arquivos extraídos, você precisará limpar o cache de distribuição e desmarcar a caixa **Permitir a distribuição adicional de programas criados a partir deste pacote de distribuição** antes de iniciar o pacote de distribuição confiável novamente.

Os arquivos e pacotes extraídos criados por um pacote primário de distribuição confiável herdam o atributo de confiabilidade quando as suas somas de verificação são adicionadas ao cache de distribuição quando o pacote de distribuição de software na lista de exclusão é aberto pela primeira vez. Portanto, o próprio pacote de distribuição e todos os arquivos extraídos desse pacote também serão confiáveis. Por padrão, o número de níveis de herança do atributo de confiabilidade é ilimitado.

Os arquivos extraídos manterão o atributo de confiabilidade após a reinicialização do sistema operacional.

O processamento de arquivos é definido nas configurações de Controle de Distribuição de Software selecionando ou desmarcando a caixa **Permitir a distribuição adicional de programas criados a partir deste pacote de distribuição**.

Por exemplo, caso o test.msi, um pacote que contém vários pacotes e aplicativos, seja adicionado à lista de exclusões e a caixa de seleção seja marcada, todos os pacotes e aplicativos contidos no pacote test.msi poderão ser descompactados e executados, mesmo se contiverem outros arquivos aninhados. 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 distribuição adicional de programas criados a partir deste pacote de distribuição**, o aplicativo definirá o atributo de confiabilidade apenas aos pacotes e arquivos executáveis extraídos diretamente do pacote confiável primário (aninhado no 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.

Trabalhar 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.

Uso das conclusões do KSN

As conclusões da KSN de que um arquivo não é confiável têm uma prioridade mais alta do que as exclusões do Controle de Distribuição de Software. A descompactação de pacotes confiáveis e a inicialização de arquivos criados ou modificados por pacotes confiáveis serão bloqueadas caso uma conclusão da KSN tenha sido recebida indicando que esses arquivos não são confiáveis.

Nesse caso, depois de serem descompactados de um pacote confiável, será permitido que todos os arquivos filhos sejam executados independentemente do uso da KSN no escopo do Controle de Inicialização de Aplicativos. Nesse caso, os estados das caixas de seleção **Negar aplicativos não confiáveis pela KSN** e **Permitir aplicativos confiáveis pela KSN** não afetam a operação da caixa de seleção **Permitir a distribuição adicional de programas criados a partir deste pacote de distribuição**.

Sobre o uso da KSN para a tarefa de Controle de Inicialização de Aplicativos

Para iniciar a tarefa de Uso da KSN, você deve aceitar a Declaração da Kaspersky Security Network.

Se os dados da KSN sobre a reputação de um aplicativo forem usados pela tarefa de Controle de Inicialização de Aplicativos, a reputação do aplicativo na KSN será considerada um critério para permitir ou negar a inicialização desse aplicativo. Se a KSN reportar para o Kaspersky Embedded Systems Security for Windows que um aplicativo não é confiável, quando o usuário tentar iniciar o aplicativo, a inicialização do aplicativo será negada. Se a KSN reportar para o Kaspersky Embedded Systems Security for Windows que um aplicativo é confiável, quando o usuário tentar iniciar o aplicativo, a inicialização do aplicativo será permitida. A KSN pode ser usada junto com as regras de Controle de Inicialização de Aplicativos ou como um critério independente para negar a inicialização de aplicativos.

Usar conclusões da KSN como critério independente para negar a inicialização do aplicativo

Este cenário permite que você controle com segurança inicializações de aplicativos em um dispositivo protegido sem a necessidade de configuração avançada da lista de regras.

É possível aplicar conclusões da KSN ao Kaspersky Embedded Systems Security for Windows em conjunto com a única regra especificada. O aplicativo só permitirá a inicialização de aplicativos confiáveis na KSN ou os permitidos por uma regra específica.

Para esse cenário, recomendamos definir uma regra que permita a inicialização do aplicativo com base em um certificado digital.

Todos os outros aplicativos serão negados conforme a política de Negação padrão. Usar a KSN quando nenhuma regra é aplicada protege um dispositivo de aplicativos que a KSN considera como uma ameaça.

Usar conclusões da KSN simultaneamente com regras de Controle de Inicialização de Aplicativos

Ao usar as conclusões da KSN simultaneamente com regras de Controle de Inicialização de Aplicativos, as seguintes condições se aplicam:

- O Kaspersky Embedded Systems Security for Windows sempre nega a inicialização de um aplicativo se este estiver incluído no escopo de ao menos uma regra de negação. Se o aplicativo for considerado confiável pela KSN, a conclusão correspondente terá uma prioridade mais baixa e não será considerada; a inicialização do aplicativo ainda será negada. Isso permite expandir a lista de aplicativos bloqueados.

- O Kaspersky Embedded Systems Security for Windows sempre nega a inicialização de um aplicativo se a inicialização de aplicativos não confiáveis na KSN for proibida e o aplicativo não for confiável na KSN. Se uma regra de permissão for definida para o aplicativo, ela terá uma prioridade mais baixa e não será considerada; a inicialização do aplicativo ainda será negada. Isso protege o dispositivo de aplicativos que a KSN considera como ameaças, mas que não foram considerados durante a configuração inicial das regras.

Sobre o Gerador de Regras de Controle de Inicialização de Aplicativos

É possível criar listas de regras de Controle de Inicialização de Aplicativos usando tarefas e políticas do Kaspersky Security Center simultaneamente para todos os dispositivos protegidos e grupos de dispositivos protegidos na rede corporativa. Estes cenários listados abaixo são recomendados se a rede corporativa não tiver uma máquina modelo e se você não puder criar uma lista de regras de permissão baseada em aplicativos instalados nesta máquina-modelo.

Você pode executar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos localmente por meio do Console do Aplicativo para criar uma lista de regras com base nos aplicativos em execução em um único dispositivo protegido.

O componente de Controle de Inicialização de Aplicativos é instalado com duas regras de permissão predefinidas:

- Regra de permissão para scripts e pacotes do Windows Installer com um certificado confiável pelo sistema operacional.
- Regra de permissão para arquivos executáveis com certificado confiável pelo 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 do Gerador de Regras de Controle de Inicialização de Aplicativos.

  Nesse cenário, uma tarefa de grupo gera sua própria lista de regras de Controle de Inicialização de Aplicativos para cada dispositivo protegido na rede e salva essas listas em um arquivo XML na pasta compartilhada especificada. O arquivo XML gerado pela tarefa Gerador de Regras de Controle de Inicialização de Aplicativos contém as regras de permissão especificadas nas configurações da tarefa antes do início da tarefa. Nenhuma regra será criada para os aplicativos que não tenham permissão para ser iniciados nas configurações de tarefa especificadas. A inicialização desses aplicativos é negada por padrão. Você pode então importar manualmente a lista de regras criada para tarefa de Controle de Inicialização de Aplicativos da política do Kaspersky Security Center.

  Você pode configurar a importação automática das regras geradas para a lista de regras da tarefa de Controle de Inicialização de Aplicativos.

  Este cenário é recomendado quando você precisar criar listas de regras de Controle de Inicialização de Aplicativos rapidamente. Recomendamos configurar a inicialização programada da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos somente se o escopo de uso das regras de permissão incluir pastas e arquivos já identificados como seguros.

  Antes de usar a tarefa de Controle de Inicialização de Aplicativos na rede, certifique-se de que todos os dispositivos protegidos tenham acesso a uma pasta compartilhada. Caso a política da organização não preveja o uso de uma pasta compartilhada na rede, recomendamos iniciar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos em um dispositivo protegido em um grupo de dispositivos protegidos de teste ou em uma máquina de referência.

- Com base em um relatório dos eventos de tarefa gerados no Kaspersky Security Center pela execução da tarefa de Controle de Inicialização de Aplicativos no modo **Somente estatísticas**.

  Nesse cenário, o Kaspersky Embedded Systems Security for Windows não nega a inicialização de aplicativos. Em vez disso, com a execução do Controle de Inicialização de Aplicativos no modo **Somente estatísticas**, ele reporta todas as inicializações de aplicativos permitidas e negadas em todos os dispositivos protegidos da rede na guia **Eventos** da área de trabalho do node Servidor de Administração no Kaspersky Security Center. O Kaspersky Security Center usa os relatórios para gerar uma lista única de eventos nos quais a inicialização de aplicativos foi negada.

Você precisa configurar o período de execução da tarefa para que todos os cenários possíveis envolvendo dispositivos protegidos e grupos de dispositivos protegidos e, ao menos uma reinicialização de dispositivo protegido sejam executados durante o período de tempo especificado. Após o final do período de execução de tarefa, você pode importar dados de inicialização do relatório de eventos do Kaspersky Security Center (no formato TXT) e gerar regras de permissão para o Controle de Inicialização de Aplicativos para esses aplicativos com base nesses dados.

Este cenário é recomendado se uma rede corporativa incluir uma grande quantidade de dispositivos protegidos de tipos diferentes (com softwares diferentes instalados).

- 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 dispositivo protegido deve estar em execução segundo uma política ativa do Kaspersky Security Center. Neste caso, todos os eventos no dispositivo protegido são enviados para o Servidor de administração.

Recomendamos que você atualize a lista de regras quando houver alterações no conjunto de aplicativos instalado nos dispositivos protegidos da rede (por exemplo, quando as atualizações são instaladas ou os sistemas operacionais são reinstalados). Recomendamos que você gere uma lista atualizada de regras executando a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos ou a tarefa de Controle de Inicialização de Aplicativos no modo **Somente estatísticas** em dispositivos protegidos no grupo de administração de teste. O grupo de administração de teste inclui dispositivos protegidos necessários para testar a inicialização de novos aplicativos antes que eles sejam instalados em dispositivos protegidos da rede.

Os arquivos de XML contendo listas de regras de permissão são criados com base em uma análise das tarefas iniciadas no dispositivo protegido. Para considerar todos os aplicativos utilizados na rede ao gerar listas de regras, aconselha-se a inicialização da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos e a tarefa de Controle de Inicialização de Aplicativos no modo **Somente estatísticas** em uma máquina modelo.

Antes de iniciar a geração das regras de permissão com base nos aplicativos iniciados em uma máquina modelo, certifique-se de que a máquina-modelo esteja segura e que não contenha nenhum malware.

Antes de acrescentar regras de permissão, selecione um dos modos de aplicação de regras disponíveis. A lista das regras da política do Kaspersky Security Center exibe apenas as regras especificadas pela política, independentemente do modo de aplicação da regra. A lista de regras locais inclui todas as regras aplicadas - tanto as regras locais como as regras adicionadas através de uma política.

Configurações padrão da tarefa de Controle de Inicialização de Aplicativos

Por padrão, a tarefa de Controle de Inicialização de Aplicativos possui as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Configurações padrão da tarefa de Controle de Inicialização de Aplicativos

Configuração	Valor padrão	Descrição
Modo da tarefa.	**Somente estatísticas**. A tarefa registra eventos de inicialização negados e permitidos com base nas regras definidas. A inicialização do aplicativo não é de fato negada.	Você pode selecionar o modo **Ativa** depois que a lista final de regras for gerada.

Repetir ação da primeira inicialização de arquivo em todas as inicializações subsequentes deste arquivo	Não aplicado	Você pode repetir ações executadas na primeira inicialização do arquivo em todas as inicializações subsequentes desse arquivo.
Negar a inicialização de interpretadores de comando sem um comando a executar	Não aplicado.	É possível negar a inicialização de interpretadores da linha de comando sem um comando a ser executado.
Gerenciamento de regras	**Adicionar regras de política às regras locais**	É possível selecionar um modo em que regras especificadas em uma política sejam aplicadas em conjunto com as regras no dispositivo protegido.
Escopo de uso da regra	A tarefa controla a inicialização de arquivos executáveis, scripts e pacotes MSI. A tarefa também monitora o carregamento de módulos DLL.	Você pode especificar os tipos de arquivos para os quais a inicialização será controlada por regras.
Uso da KSN	Os dados de reputação do aplicativo na KSN não serão utilizados.	É possível usar os dados da reputação do aplicativo da KSN ao executar uma tarefa de Controle de Inicialização de Aplicativos.
Permitir automaticamente a distribuição de software por meio dos 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. Pode ser alterado apenas quando a configuração **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados** estiver ativa.	É possível permitir qualquer instalação ou atualização de software se as operações forem executadas por meio do Windows Installer.
Sempre permitir distribuição de software via SCCM usando o Background Intelligent Transfer Service	Não aplicado. Pode ser alterado apenas quando a configuração **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados** estiver ativa.	Você pode ativar ou desativar a distribuição automática de software usando o System Center Configuration Manager.
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 for Windows. É possível iniciar a tarefa manualmente ou configurar um início programado.

Configurações padrão da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

Configuração	Valor padrão	Descrição
Prefixo para	Idêntico ao nome do dispositivo	Você pode modificar o prefixo dos nomes de regras

nomes de regras de permissão	protegido no qual o Kaspersky Embedded Systems Security for Windows está instalado.	de permissão.
Escopo de uso das regras de permissão	O escopo de uso das regras de permissão inclui as seguintes categorias de arquivos por padrão: • Arquivos com a extensão EXE localizados nas pastas C:\Windows, C:\Program Files (x86) e C:\Program Files • Pacotes MSI armazenados na pasta C:\Windows • Scripts armazenados na pasta C:\Windows A tarefa também cria regras para todos os aplicativos em execução, independente de seu local e formato.	Você pode modificar o escopo de proteção adicionando ou removendo caminhos de pastas e especificando tipos de arquivo que poderão ser inicializados pelas regras geradas automaticamente. Você também pode ignorar os aplicativos em execução ao criar regras de permissão.
Critérios para a geração de regras de permissão	O requerente e a impressão digital do certificado digital serão usados; as regras serão geradas para todos os usuários e grupos de usuários.	Você pode usar o Hash SHA256 gerando regras de permissão. Você pode selecionar um usuário e grupo de usuários para os quais as regras de permissão devem ser geradas automaticamente.
Ações após a conclusão da tarefa	As regras de permissão são adicionadas à lista de regras de Controle de Inicialização de Aplicativos; as novas regras serão agregadas às existentes; as regras duplicadas serão removidas.	Você pode adicionar regras às regras existentes sem agregá-las e sem excluir regras duplicadas, ou substituir as regras existentes por regras novas de permissão ou configurar a exportação de regras de permissão para um arquivo.
Configurações de inicialização de tarefa com permissões	A tarefa é iniciada em uma conta do sistema.	Você pode permitir a inicialização da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos através de uma conta do sistema ou das permissões de um usuário especificado.
Programação de inicialização da tarefa	A primeira execução não está programada.	A tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos não é iniciada automaticamente no momento da inicialização do Kaspersky Embedded Systems Security for Windows. É possível iniciar a tarefa manualmente ou configurar um início programado.

Gerenciamento do Controle de Inicialização de Aplicativos por meio do Plug-in de Administração

Nesta seção, saiba como navegar pela interface do Plug-in de Administração e definir configurações de tarefa para um ou todos os dispositivos protegidos na rede.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das definições de política para a tarefa de Controle de Inicialização de Aplicativos

Para abrir as configurações da tarefa de Controle de Inicialização de Aplicativos por meio da política no Kaspersky Security Center:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Controle de atividades locais**.
6. Clique no botão **Configurações** na subseção **Controle de inicialização de aplicativos**.
   A janela **Controle de Inicialização de Aplicativos** é exibida.

Configure a política conforme necessário.

Abertura da lista de regras de Controle de Inicialização de Aplicativos

Para abrir a lista de regras de Controle de Inicialização de Aplicativos por meio do Kaspersky Security Center:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Controle de atividades locais**.
6. Clique no botão **Configurações** na subseção **Controle de inicialização de aplicativos**.
   A janela **Controle de Inicialização de Aplicativos** é exibida.
7. Na guia **Geral**, clique no botão **Lista de regras**.
   A janela **Regras de Controle de Inicialização de Aplicativos** é exibida.

Configure a lista de regras conforme necessário.

Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

Para criar uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Abra a guia **Tarefas**.
4. Clique no botão **Nova tarefa**.

   A janela **Assistente de Nova Tarefa** será aberta.
5. Selecione a tarefa **Gerador de Regras de Controle de Inicialização de Aplicativos**.
6. Clique no botão **Avançar**.

   A janela **Configurações** é exibida.

Para configurar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Abra a guia **Tarefas**.
4. Clique duas vezes no nome da tarefa na lista de tarefas no Kaspersky Security Center.

   A janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos** é exibida.

Consulte a seção Configuração da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos para detalhes sobre a configuração da tarefa.

Definição de configurações da tarefa de Controle de Inicialização de Aplicativos

Para definir as configurações gerais da tarefa de Controle de Inicialização de Aplicativos:

1. Abra a janela **Controle de Inicialização de Aplicativos**.
2. Na guia **Geral**, selecione as seguintes configurações na seção **Modo da tarefa**:
   - Na lista suspensa **Modo da tarefa**, especifique o modo da tarefa.
   - Desmarque ou marque a caixa de seleção **Repetir ação da primeira inicialização de arquivo em todas as inicializações subsequentes deste arquivo**.

- Desmarque ou marque **Negar a inicialização de interpretadores de comando sem um comando a executar**.

3. No bloco **Gerenciamento de regras**, defina as configurações para a aplicação de regras:

   a. Clique no botão **Lista de regras** para adicionar as regras de permissão para a tarefa de Controle de Inicialização de Aplicativos.

   > O Kaspersky Embedded Systems Security for Windows 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 de Inicialização de Aplicativos centralizado em um grupo de dispositivos protegidos. 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 a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos.

4. Na seção **Escopo de uso da regra**, especifique as seguintes configurações:

   - **Aplicar regras a arquivos executáveis**.
   - **Monitorar o carregamento de módulos DLL**.

     > O controle do carregamento de módulos DLL pode afetar o desempenho do sistema operacional.

   - **Aplicar regras a scripts e pacotes MSI**.

5. No grupo **Uso da KSN**, defina as seguintes configurações de inicialização de aplicativos:

   - **Negar aplicativos não confiáveis pela KSN**.
   - **Permitir aplicativos confiáveis pela KSN**.
   - Os usuários e/ou grupos de usuário permitiram a inicialização de aplicativos confiáveis na KSN:

     a. No menu de contexto do botão **Editar**, selecione o método para adicionar usuários.

     A janela **Selecionar usuário ou grupo de usuários** é aberta.

     b. Selecione um usuário ou grupo de usuários.

     c. Clique no botão **OK**.

6. Na guia **Controle de distribuição de software**, defina as configurações do controle de distribuição de software.

7. Na guia **Gerenciamento da tarefa** defina as configurações de programação de inicialização da tarefa.

8. Clique no botão **OK** na janela **Controle de Inicialização de Aplicativos**.

O Kaspersky Embedded Systems Security for Windows aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Configuração do controle de distribuição de software

Para adicionar um pacote de distribuição confiável pelo Plug-in de Administração:

1. Abra a janela **Controle de Inicialização de Aplicativos**.
2. Na guia **Controle de distribuição de software**, marque a caixa de seleção **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados**.

   É possível selecionar **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados** se a caixa de seleção **Controle de Inicialização de Aplicativos** na guia **Aplicar regras a arquivos executáveis** estiver marcada nas configurações da tarefa de **Geral**.

3. Desmarque a caixa de seleção **Sempre permitir distribuição de software via Windows Installer**, se necessário.

   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 de arquivos do sistema operacional e também impedir a inicialização de arquivos extraídos de um pacote de distribuição.

4. Se necessário, marque a caixa de seleção **Sempre permitir distribuição de software via SCCM usando o Background Intelligent Transfer Service**.

   O aplicativo controla o ciclo de distribuição de software no dispositivo protegido, da entrega do pacote à instalação ou atualização. O aplicativo não controla processos se algum dos estágios da distribuição tiver sido executado antes da instalação do aplicativo no dispositivo protegido.

5. Para criar uma lista de permissão ou 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**.

     b. Selecione o arquivo executável ou pacote de distribuição.

     O bloco **Critérios de confiança** é automaticamente preenchido com os dados sobre o arquivo selecionado.

     c. Desmarque ou marque a caixa **Permitir a distribuição adicional de programas criados a partir deste pacote de distribuição**.

     d. 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**
- **Usar hash SHA256**

- **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 for Windows 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.

  Na janela **Abrir**, especifique o arquivo de configuração que contém uma lista de pacotes de distribuição confiáveis.

Caso um pacote de distribuição confiável seja criado de acordo com um arquivo executável, um processo tenha sido adicionado nas configurações da Zona Confiável de acordo com esse mesmo arquivo executável e esse arquivo tenha se tornado confiável para a tarefa Controle de Inicialização de Aplicativos, as configurações da Zona Confiável terão uma prioridade mais alta. O Kaspersky Embedded Systems Security for Windows bloqueia a inicialização desse arquivo executável, mas considera o processo do arquivo executável como confiável.

6. Caso queira 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 dispositivo protegido ou crie uma regra de negação nas configurações da tarefa de Controle de Inicialização de Aplicativos.

7. Clique no botão **OK**.

As configurações especificadas são salvas.

Configuração de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

Para configurar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Abra a janela Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos.
2. 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*.

3. Na seção **Configurações**, é possível definir as seguintes configurações:

   - Especifique um prefixo para nomes de regra.
   - Selecione como criar as regras de permissão:
     - Criar regras de permissão com base nos aplicativos em execução
     - Criar regras de permissão para aplicativos das pastas

4. Na seção **Opções**, é possível especificar ações para execução ao criar regras de permissão para o controle de inicialização de aplicativos:

   - Usar certificado digital
   - Usar assunto e miniatura do certificado digital
   - Se o certificado estiver ausente, usar
     - **Hash SHA256**. O valor da soma de verificação do arquivo usado para gerar a regra é estabelecido como o critério para acionamento da regra 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 da regra de permissão de Controle de Inicialização de Aplicativos. O aplicativo agora permitirá a inicialização de programas usando arquivos localizados nas pastas especificadas na tabela **Criar regras de permissão para aplicativos das pastas** na seção **Configurações**.
   - Usar hash SHA256
   - Gerar regras para usuário ou grupo de usuários.

   É possível definir as configurações para os arquivos de configuração com as listas de regras de permissão para o Controle de Dispositivos e o Controle de Inicialização de Aplicativos. O Kaspersky Embedded Systems Security for Windows cria essas listas quando a tarefa é concluída.

5. Configure a programação da tarefa na seção **Agendamento** (é possível configurar uma programação para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).

6. Na seção **Conta**, especifique a conta cujos direitos serão usados para executar a tarefa.

7. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

   Para obter informações detalhadas sobre as definições das configurações nessas seções, consulte a *Ajuda do Kaspersky Security Center*.

8. Clique no botão **OK** na janela **Propriedades: <Nome da tarefa>**.

   As recém-definidas configurações da tarefa de grupo são salvas.

Configuração de regras de Controle de Inicialização de Aplicativos por meio do Kaspersky Security Center

Saiba como gerar uma lista de regras com base em vários critérios ou criar regras de permissão ou negação manualmente usando a tarefa de Controle de Inicialização de Aplicativos.

Adição de uma regra de Controle de Inicialização de Aplicativos

Para adicionar uma regra de Controle de Inicialização de Aplicativos usando o Plug-in de Administração:

1. Abra a janela **Regras de Controle de Inicialização de Aplicativos**.
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão, selecione **Adicionar uma regra**.
   A janela **Configurações de regra** é exibida.
4. Especifique as seguintes configurações:
   a. No campo **Nome**, digite o nome da regra.
   b. Na lista suspensa **Tipo**, selecione o tipo de regra:
      - **Permissão**, se quiser que a regra permita a inicialização de aplicativos de acordo com os critérios especificados nas configurações da regra.
      - **Proibição**, se quiser que a regra bloqueie a inicialização dos aplicativos de acordo com os critérios especificados nas configurações da regra.
   c. Na lista suspensa **Escopo**, selecione o tipo de arquivo cuja execução será controlada pela regra:
      - **Arquivos executáveis**, se quiser que a regra controle a inicialização de arquivos executáveis.
      - **Pacotes de scripts e MSI**, se quiser que a regra controle a inicialização de scripts e pacotes MSI.
   d. No campo **Usuário ou grupo de usuários**, especifique os usuários que terão permissão ou não para iniciar programas de acordo com o tipo da regra.
      1. No menu de contexto do botão **Procurar**, selecione o método para adicionar usuários confiáveis.
         A janela **Seleção de usuário ou grupo de usuários** é aberta.
      2. Selecione um usuário ou grupo de usuários.
      3. Clique no botão **OK**.
   e. Caso queira obter os valores dos critérios para acionamento de regras listados no bloco **Critério para acionamento da regra** a partir de um arquivo, faça o seguinte:
      1. Clique no botão **Definir critério para acionamento de regras a partir das propriedades do arquivo**.

A janela **Abrir** padrão do Microsoft Windows é exibida.

2. Selecione o arquivo.

3. Clique no botão **Abrir**.

   O valor dos critérios no arquivo é exibido nos campos no bloco **Critério para acionamento da regra**. O critério para o qual os dados estão disponíveis nas propriedades de arquivo é selecionado por padrão.

f. Na caixa do grupo **Critério para acionamento da regra**, selecione uma ou várias das seguintes opções:

- **Certificado digital**, se quiser que a regra controle a inicialização de programas que usam arquivos assinados com um certificado digital:
  - Marque a caixa de seleção **Usar assunto** se quiser que a regra controle a inicialização de arquivos assinados com um certificado digital somente com o requerente especificado.
  - Marque a caixa de seleção **Usar miniatura** se você quiser que a regra controle a inicialização de arquivos assinados com um certificado digital somente com a impressão digital especificada.
- **Hash SHA256**, se quiser que a regra controle a inicialização de programas que usam os arquivos cuja soma de verificação corresponda àquela especificada.
- **Caminho do arquivo**, se quiser que a regra controle a inicialização de programas que usam os arquivos localizados no caminho especificado.
  - **Linha de comando** se desejar que a regra controle o início de programas iniciados usando os argumentos especificados no campo de linha de comando. O campo é ativado após selecionar a opção **Caminho para o arquivo**. É possível usar os caracteres ? e * como uma máscara ao especificar os argumentos da linha de comando para processos iniciados como um critério.

> O Kaspersky Embedded Systems Security for Windows não reconhece caminhos que contêm barras ("/"). Use a barra invertida ("\") para inserir o caminho corretamente.

> Ao especificar os objetos, você pode usar ? e * caracteres como máscaras de arquivo.

É preciso selecionar ao menos uma opção. Caso contrário, a regra de Controle de Inicialização de Aplicativos não será adicionada.

g. Se deseja adicionar exclusões de regra:

1. Na seção **Exclusões da regra**, clique no botão **Adicionar**.

   A janela **Exclusão da regra** é exibida.

2. No campo **Nome**, digite o nome da exclusão.

3. Especifique as configurações para exclusão dos arquivos de aplicativos da regra de Controle de Inicialização de Aplicativos. Você pode preencher os campos de configurações a partir das propriedades do arquivo clicando no botão **Definir exclusão com base nas propriedades do arquivo**.

   - Certificado digital
   - Usar assunto

- Usar miniatura
- Hash SHA256
- Caminho do arquivo

4. Clique no botão **OK**.
5. Se necessário, repita os itens (i)-(iv) para incluir exclusões adicionais.

5. Clique no botão **OK** na janela **Configurações de regra**.

A regra criada é exibida na lista na janela **Regras de Controle de Inicialização de Aplicativos**.

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 da KSN de que não são confiáveis. O modo de Permissão padrão pode ser ativado adicionando regras de permissão específicas. Você pode ativar a Permissão padrão apenas para scripts ou para todos os arquivos executáveis.

Para adicionar uma regra de Permissão padrão:

1. Abra a janela Regras de Controle de Inicialização de Aplicativos.
2. Clique no botão **Adicionar** e, no menu de contexto do botão, selecione a opção **Adicionar uma regra**.
   A janela **Configurações de regra** é exibida.
3. No campo **Nome**, digite o nome da regra.
4. Na lista suspensa **Tipo**, selecione o tipo de regra **Permissão**.
5. Na lista suspensa **Escopo**, selecione o tipo de arquivo cuja execução será controlada pela regra:
   - **Arquivos executáveis**, se quiser que a regra controle a inicialização de arquivos executáveis.
   - **Pacotes de scripts e MSI**, se quiser que a regra controle a inicialização de scripts e pacotes MSI.
6. No grupo **Critério para acionamento da regra**, selecione a opção **Caminho do arquivo**.
7. Insira a seguinte máscara: `?:\`
8. Clique no botão **Configurações de regra** na janela **OK**.

O Kaspersky Embedded Systems Security for Windows aplicará o modo de Permissão padrão.

Criação de regras de permissão para o controle de inicialização de aplicativos nos eventos do Kaspersky Security Center

Para criar regras de permissão para o controle de inicialização de aplicativos a partir de eventos do Kaspersky Security Center:

1. Abra a janela Regras de Controle de Inicialização de Aplicativos.
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão, selecione **Criar regras de permissão para aplicativos de eventos do Kaspersky Security Center**.
4. Selecione o princípio para adicionar as regras à lista de regras de Controle de Inicialização de Aplicativos criadas anteriormente:

   - **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
   - **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas.
   - **Mesclar com as regras existentes**, se quiser adicionar as regras importadas à lista de 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 **Geração de regras de controle de inicialização de aplicativos** é exibida.
5. Selecione os tipos de eventos de acordo com os quais o aplicativo criará regras de controle de inicialização de aplicativos:

   - **Modo somente estatísticas: inicialização de aplicativos negada**.
   - **Inicialização do aplicativo negada**.
6. Selecione o período de tempo na lista suspensa **Solicitação de eventos que foram gerados dentro do período**.
7. Caso necessário, no campo **Usar os eventos gerados para um grupo de dispositivos gerenciados**, insira o nome ou um fragmento do nome do grupo de dispositivos gerenciados pelo Kaspersky Security Center cujos eventos serão a base para a criação de regras de controle de inicialização de aplicativos.
8. Desmarque ou marque a caixa de seleção Priorizar o uso de hash ao gerar regras.

   Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security for Windows usa a soma de verificação do arquivo para gerar a regra quando a soma de verificação e o certificado do arquivo estiverem disponíveis.

   Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows usa o certificado digital do arquivo para gerar a regra quando a soma de verificação e o certificado do arquivo estiverem disponíveis.
9. Clique no botão **Gerar regras**.
10. Clique no botão **Salvar** na janela **Regras de Controle de Inicialização de Aplicativos**.

    A lista de regras na tarefa de Controle de Inicialização de Aplicativos será preenchida com as novas regras geradas com base em dados do sistema do dispositivo protegido com o Console de Administração do Kaspersky Security Center instalado.

    As regras com o mesmo hash não serão adicionadas, pois todas as regras em uma lista devem ser únicas.

Importação de regras a partir de um relatório do Kaspersky Security Center sobre aplicativos bloqueados

Você pode importar dados sobre inicializações bloqueadas de aplicativos a partir do relatório gerado no Kaspersky Security Center após a conclusão da tarefa 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 ocorridos durante a execução da tarefa de Controle de Inicialização de Aplicativos, você pode acompanhar os aplicativos cuja inicialização foi bloqueada.

Ao importar dados do relatório sobre aplicativos bloqueados para as definições da política, certifique-se de que a lista que está sendo usada contém somente aplicativos cuja inicialização você deseja permitir.

Para especificar regras de permissão de Controle de Inicialização de Aplicativos para um grupo de dispositivos protegidos com base no relatório de aplicativos bloqueados do Kaspersky Security Center:

1. Abra a janela **Controle de Inicialização de Aplicativos**.
2. No bloco **Modo da tarefa**, selecione o modo **Somente estatísticas**.
3. Nas propriedades da política, na seção **Notificação de evento**, certifique-se de que:
   - Para eventos **críticos**, o período de retenção do log de tarefas para eventos de **Inicialização do aplicativo negada** excede o período planejado para a execução da tarefa no modo **Somente estatísticas** (o valor padrão é 30 dias).
   - Para eventos com um nível de importância de **Aviso**, o período de retenção do log de tarefas para eventos do **Modo somente estatísticas: inicialização de aplicativos negada** excede o período planejado para a execução da tarefa no modo **Somente estatísticas** (o valor padrão é 30 dias).

     Quando o período de retenção para eventos é excedido, as informações sobre os eventos registrados são excluídas e não são refletidas no 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 configurado para os eventos especificados.
4. Quando a tarefa tiver sido concluída, exporte os eventos registrados para um arquivo TXT:
   a. Na área de trabalho do node **Servidor de Administração** no Kaspersky Security Center, selecione a guia **Eventos**.
   b. Clique no botão **Criar uma seleção** para criar uma seleção de eventos com base no critério Bloqueado para visualizar os aplicativos cujo início será bloqueado pela tarefa de Controle de Inicialização de Aplicativos.
   c. No painel de resultados da seleção, clique em **Exportar eventos para o arquivo** para salvar o relatório de inicializações bloqueadas de aplicativos em um arquivo TXT.

Antes de importar e aplicar o relatório gerado a uma política, certifique-se de que o relatório contém dados somente sobre aqueles aplicativos cuja inicialização você deseja permitir.

5. 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 adição de regras da lista criada com base em um relatório do Kaspersky Security Center à lista de regras previamente configuradas de Controle de Inicialização de Aplicativos:

   - **Mesclar com as regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas não são duplicadas. Se pelo menos uma configuração de regra for exclusiva, a regra será adicionada.

   - **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.

   a. **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas. Na janela padrão do Microsoft Windows exibida, selecione o arquivo TXT para o qual os eventos do relatório de inicializações bloqueadas de aplicativos foram exportados.

   b. Clique no botão **Salvar** na janela **Regras de Controle de Inicialização de Aplicativos**.

As regras criadas com base no relatório do Kaspersky Security Center sobre aplicativos bloqueados serão adicionadas à lista de regras de controle de inicialização de aplicativos.

Importação de regras de Controle de Inicialização de Aplicativos de um arquivo XML

Você pode importar relatórios gerados após a conclusão da tarefa de grupo do 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 do 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 compartilhada especificada. Cada arquivo com a lista de regras é criado com base na análise de arquivos executados e aplicativos iniciados em cada dispositivo protegido separado na rede corporativa. As listas contêm regras de permissão para arquivos e aplicativos cujo tipo corresponde ao tipo especificado na tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos.

Para especificar regras de permissão de Controle de Inicialização de Aplicativos para um grupo de dispositivos protegidos com base em uma lista de regras de permissão gerada automaticamente:

1. Na guia **Tarefas**, no painel de detalhes do grupo de dispositivos protegidos que você está configurando, crie uma Tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos ou selecione uma tarefa existente.

2. Nas propriedades da tarefa de grupo do 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 informações 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 conjunto de pastas que contêm aplicativos permitidos: exclua as pastas padrão do escopo da tarefa ou adicione novas pastas manualmente.
- Na seção **Opções**, especifique as operações a serem executadas pela tarefa durante a sua execução e após a sua conclusão. Especifique o critério com base no qual as regras serão geradas e o nome do arquivo para o qual essas regras serão exportadas.
- Na seção **Agendamento**, defina as configurações da programação de 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 dispositivos protegidos a serem excluídos do escopo da tarefa.

O Kaspersky Embedded Systems Security for Windows não criará regras de permissão para aplicativos iniciados em dispositivos protegidos excluídos.

3. Na guia **Tarefas** no painel de detalhes do grupo de dispositivos protegidos sendo configurados, na lista de tarefas de grupo selecione a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos que você criou e clique no botão **Iniciar** para iniciar a tarefa.

   Quando a tarefa for concluída, as listas de regras de permissão geradas automaticamente serão salvas em arquivos XML em uma pasta compartilhada.

Antes de usar a tarefa de Controle de Inicialização de Aplicativos na rede, certifique-se de que todos os dispositivos protegidos tenham acesso a uma pasta compartilhada. Se a política da organização não prevê o uso de uma pasta compartilhada na rede, recomendamos que você inicie a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos em um dispositivo protegido em um grupo de dispositivos protegidos de teste ou em uma máquina de referência.

4. Para adicionar as listas de regras de permissão geradas à tarefa de Controle de Inicialização de Aplicativos:

   a. Abra a janela Regras de Controle de Inicialização de Aplicativos.

   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:

   - **Mesclar com as regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas não são duplicadas. Se pelo menos uma configuração de regra for exclusiva, a regra será adicionada.
   - **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
     - **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas.

a. Na janela padrão do Microsoft Windows, selecione os arquivos XML criados após a conclusão da tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos.

b. Clique no botão **Salvar** na janela **Regras de Controle de Inicialização de Aplicativos**.

5. Se você quiser aplicar as regras criadas para controlar a inicialização de aplicativos, na política nas propriedades da tarefa de Controle de Inicialização de Aplicativos, selecione o modo **Ativa** para a tarefa.

Regras de permissão geradas automaticamente com base em execuções de tarefa em cada dispositivo protegido separado são aplicadas a todos os dispositivos protegidos de rede abrangidos pela política que está sendo configurada. Nesses dispositivos protegidos, o aplicativo permitirá a inicialização somente daqueles aplicativos para os quais foram criadas regras de permissão.

Verificação da inicialização de aplicativos

Antes de aplicar as regras de Controle de Inicialização de Aplicativos configuradas, você pode testar qualquer aplicativo para determinar quais regras de Controle de Inicialização de Aplicativos são acionadas pelo aplicativo.

O Kaspersky Embedded Systems Security for Windows nega a inicialização de aplicativos cuja inicialização não é permitida por uma única regra. Para evitar a negação da inicialização de aplicativos importantes você deve criar regras de permissão para eles.

Se a inicialização do aplicativo for controlada por várias regras de tipos diferentes, as regras de negação têm prioridade: a inicialização do aplicativo será negada se cair em ao menos uma regra de negação.

Para testar as regras de Controle de Inicialização de Aplicativos:

1. Abra a janela **Regras de Controle de Inicialização de Aplicativos**.

2. Na janela exibida, clique no botão **Mostrar regras do arquivo**.

   A janela padrão do Microsoft Windows é exibida.

3. Selecione o arquivo cujo controle de inicialização você deseja testar.

O caminho do arquivo especificado é exibido no campo de pesquisa. A lista contém todas as regras que serão acionadas na inicialização do arquivo selecionado.

Criação de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

Para criar e configurar as definições da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Abra a janela **Configurações** no Assistente para Novas Tarefas.

2. Defina as seguintes configurações:

   - Especifique um Prefixo para nome de regras.
   - Configuração do escopo de uso das regras de permissão.

3. Clique no botão **Avançar**.

4. Especifique as ações que devem ser executadas pelo Kaspersky Embedded Systems Security for Windows:

- ao gerar regras de permissão
- ao concluir uma tarefa

5. Na janela **Agendamento**, especifique as configurações da programação de inicialização da tarefa.
6. Clique no botão **Avançar**.
7. Na janela **Seleção de uma conta para a execução da tarefa**, especifique a conta que deseja usar.
8. Clique no botão **Avançar**.
9. Especifique um nome de tarefa.
10. Clique no botão **Avançar**.

    O nome da tarefa não deve ter mais de 100 caracteres e não pode conter os seguintes símbolos: " * < > & \ : |

    A janela **Concluir a criação da tarefa** é exibida.
11. Você também pode executar a tarefa após a finalização do Assistente marcando a caixa de seleção **Executar a tarefa após a finalização do Assistente**.
12. Clique em **Concluir** para concluir a criação da tarefa.

Para configurar uma regra existente no Kaspersky Security Center,

abra a janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos** e defina as configurações descritas acima.

As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Restrição do escopo de uso da tarefa

Para restringir o escopo da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Abra a janela **Propriedades:Gerador de Regras de Controle de Inicialização de Aplicativos**.
2. Selecione como criar as regras de permissão:
   - **Criar regras de permissão com base nos aplicativos em execução**
   - **Criar regras de permissão para aplicativos das pastas**
3. Clique no botão **OK**.

As configurações especificadas são salvas.

Ações a serem executadas durante a geração automática de regras

Para configurar as ações que o Kaspersky Embedded Systems Security for Windows deverá executar enquanto a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos estiver sendo executada:

1. Abra a janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos**.
2. Abra a guia **Opções**.
3. No bloco **Ao gerar regras de permissão**, defina as seguintes configurações:
   - **Usar certificado digital**
   - **Usar assunto e miniatura do certificado digital**
   - **Se o certificado estiver ausente, usar**
     - **Hash SHA256**. O valor da soma de verificação do arquivo usado para gerar a regra é estabelecido como o critério para acionamento da regra 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 da regra de permissão de Controle de Inicialização de Aplicativos. O aplicativo agora permitirá a inicialização de programas usando arquivos localizados nas pastas especificadas na tabela **Criar regras de permissão para aplicativos das pastas** na seção **Configurações**.
   - **Usar hash SHA256**
   - **Gerar regras para usuário ou grupo de usuários**.
4. Clique no botão **OK**.

As configurações especificadas são salvas.

Ações a serem executadas após a conclusão da geração automática de regras

Para configurar as ações a serem executadas pelo Kaspersky Embedded Systems Security for Windows após a execução da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Abra a janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos**.
2. Abra a guia **Opções**.
3. No bloco **Após a conclusão da tarefa**, defina as seguintes configurações:
   - **Adicionar regras de permissão à lista de regras de Controle de Inicialização de Aplicativos**.
   - **Princípio da adição**.
   - **Exportar regras de permissão para o arquivo**.

- Adicionar os detalhes do dispositivo protegido ao nome do arquivo.

4. Clique no botão **OK**.

As configurações especificadas são salvas.

Gerenciamento do Controle de Inicialização de Aplicativos por meio do Console do Aplicativo

Nesta seção, aprenda a navegar pela interface do Console do Aplicativo e definir as configurações de tarefa em um dispositivo protegido.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das configurações da tarefa de Controle de Inicialização de Aplicativos

Para definir as configurações gerais da tarefa de Controle de inicialização de Aplicativos por meio do Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o nó **Controle do Computador**.
2. Selecione o nó filho **Controle de Inicialização de Aplicativos**.
3. No painel de detalhes do nó filho **Controle de Inicialização de Aplicativos**, clique no link **Propriedades**.

   A janela **Configurações de tarefa** é aberta.

Abertura da janela de regras de Controle de Inicialização de Aplicativos

Para abrir a lista de regras de Controle de Inicialização de Aplicativos por meio do Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o node **Controle do Computador**.
2. Selecione o node secundário **Controle de Inicialização de Aplicativos**.
3. No painel de resultados do node **Controle de Inicialização de Aplicativos**, clique no link **Regras de Controle de Inicialização de Aplicativos**.

   A janela **Regras de Controle de Inicialização de Aplicativos** é exibida.
4. Configure a lista de regras conforme necessário.

Abertura das definições da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

Para configurar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Na árvore do Console do Aplicativo, expanda o node **Geradores de regras automatizadas**.
2. Selecione o node secundário **Gerador de Regras de Controle de Inicialização de Aplicativos**.
3. No painel de resultados do node secundário **Gerador de Regras de Controle de Inicialização de Aplicativos**, clique no link **Propriedades**.

   A janela **Configurações de tarefa** é aberta.
4. Configure a tarefa conforme necessário.

Definição de configurações da tarefa de Controle de Inicialização de Aplicativos

Para definir as configurações gerais da tarefa de Controle de Inicialização de Aplicativos:

1. Abra a janela **Configurações de tarefa**.
2. Defina as seguintes configurações da tarefa:
   - Na guia **Geral**:
     - Modo da tarefa de Controle de Inicialização de Aplicativos.
     - Escopo de uso das regras na tarefa.
     - Uso da KSN.
   - Configurações do Controle de Distribuição de Software na guia **Controle de distribuição de software**.
   - Configurações da programação de inicialização da tarefa nas guias **Agendamento** e **Avançado**.
3. Clique em **OK** na janela **Configurações de tarefa**.

   As configurações modificadas são salvas.

O Kaspersky Embedded Systems Security for Windows aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Seleção do modo da tarefa de Controle de Inicialização de Aplicativos

Para configurar o modo da tarefa de Controle de Inicialização de Aplicativos:

1. Abra a janela **Configurações de tarefa**.
2. Na guia **Geral**, na lista suspensa **Modo da tarefa**, especifique o modo da tarefa.
3. Desmarque ou marque a caixa de seleção **Repetir ação da primeira inicialização de arquivo em todas as inicializações subsequentes deste arquivo**.

   O Kaspersky Embedded Systems Security for Windows cria uma nova lista de eventos em cache sempre que as configurações da tarefa de Controle de Inicialização de Aplicativos forem modificadas. Isso significa que o Controle de Inicialização de Aplicativos é executado de acordo com as configurações de segurança atuais.

4. Desmarque ou marque **Negar a inicialização de interpretadores de comando sem um comando a executar**.
5. Clique em **OK** na janela **Configurações de tarefa**.

As configurações especificadas são salvas.

Todas as tentativas de iniciar aplicativos são registradas no log de tarefas.

Configuração do escopo da tarefa de Controle de Inicialização de Aplicativos

Para definir o escopo da tarefa de Controle de Inicialização de Aplicativos:

1. Abra a janela **Configurações de tarefa**.
2. Na guia **Geral**, no bloco **Escopo de uso da regra**, especifique as seguintes configurações:
   - **Aplicar regras a arquivos executáveis**
   - **Monitorar o carregamento de módulos DLL**

     O controle do carregamento de módulos DLL pode afetar o desempenho do sistema operacional.

   - **Aplicar regras a scripts e pacotes MSI**
3. Clique em **OK** na janela **Configurações de tarefa**.

As configurações especificadas são salvas.

Configuração do uso da KSN

Para configurar o uso dos serviços da KSN na tarefa de Controle de Inicialização de Aplicativos:

1. Abra a janela **Configurações de tarefa**.

2. Na guia **Geral**, no bloco **Uso da KSN**, especifique as configurações para uso dos serviços da KSN:

   - Se necessário, marque a caixa de seleção **Negar aplicativos não confiáveis pela KSN**.
   - Se necessário, marque a caixa de seleção **Permitir aplicativos confiáveis pela KSN**.
   - Se a caixa de seleção **Permitir aplicativos confiáveis pela KSN** for marcada, indique os usuários e/ou grupos de usuários que podem iniciar aplicativos confiáveis na KSN. Para isso, execute as seguintes ações:

     a. Clique no botão **Editar**.

     A janela **Selecionar usuários ou grupos** padrão do Microsoft Windows é exibida.

     > Por padrão, o acesso a programas confiáveis na KSN é permitido a todos os usuários.

     b. Especifique a lista usuário e/ou grupos usuário.

     c. Clique no botão **OK**.

3. Clique em **OK** na janela **Configurações de tarefa**.

As configurações especificadas são salvas.

Configuração do controle de distribuição de software

Para adicionar um pacote de distribuição confiável pelo Console do Aplicativo:

1. Abra a janela **Configurações de tarefa**.
2. Na guia **Controle de distribuição de software**, marque a caixa de seleção **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados**.

   > É possível selecionar **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados** se a caixa de seleção **Controle de Inicialização de Aplicativos** na guia **Aplicar regras a arquivos executáveis** estiver marcada nas configurações da tarefa de **Geral**.

3. Desmarque a caixa de seleção **Sempre permitir distribuição de software via Windows Installer**, se necessário.

   > 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 de arquivos do sistema operacional e também impedir a inicialização de arquivos extraídos de um pacote de distribuição.

4. Se necessário, marque a caixa de seleção **Sempre permitir distribuição de software via SCCM usando o Background Intelligent Transfer Service**.

   > O aplicativo controla o ciclo de distribuição de software no dispositivo protegido, da entrega do pacote à instalação ou atualização. O aplicativo não controla processos se algum dos estágios da distribuição tiver sido executado antes da instalação do aplicativo no dispositivo protegido.

5. Para criar uma lista de permissão ou 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**.

     b. Selecione o arquivo executável ou pacote de distribuição.

     O bloco **Critérios de confiança** é automaticamente preenchido com os dados sobre o arquivo selecionado.

     c. Desmarque ou marque a caixa **Permitir a distribuição adicional de programas criados a partir deste pacote de distribuição**.

     d. 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**
     - **Usar hash SHA256**

   - **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 for Windows 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.

     Na janela **Abrir**, especifique o arquivo de configuração que contém uma lista de pacotes de distribuição confiáveis.

   Caso um pacote de distribuição confiável seja criado de acordo com um arquivo executável, um processo tenha sido adicionado nas configurações da Zona Confiável de acordo com esse mesmo arquivo executável e esse arquivo tenha se tornado confiável para a tarefa Controle de Inicialização de Aplicativos, as configurações da Zona Confiável terão uma prioridade mais alta. O Kaspersky Embedded Systems Security for Windows bloqueia a inicialização desse arquivo executável, mas considera o processo do arquivo executável como confiável.

6. Caso queira 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 dispositivo protegido ou crie uma regra de negação nas configurações da tarefa de Controle de Inicialização de Aplicativos.

7. Clique no botão **OK**.

As configurações especificadas são salvas.

Configuração de regras de Controle de Inicialização de Aplicativos

Aprenda como gerar, importar e exportar uma lista de regras ou criar manualmente regras de permissão ou de negação permitindo usando a tarefa de Controle de Inicialização de Aplicativos.

Adição de uma regra de Controle de Inicialização de Aplicativos

Para adicionar uma regra de Controle de Inicialização de Aplicativos usando o Console do Aplicativo:

1. Abra a janela **Regras de Controle de Inicialização de Aplicativos**.
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão, selecione **Adicionar uma regra**.

   A janela **Configurações de regra** é exibida.
4. Especifique as seguintes configurações:
   a. No campo **Nome**, digite o nome da regra.
   b. Na lista suspensa **Tipo**, selecione o tipo de regra:
      - **Permissão**, se quiser que a regra permita a inicialização de aplicativos de acordo com os critérios especificados nas configurações da regra.
      - **Proibição**, se quiser que a regra bloqueie a inicialização dos aplicativos de acordo com os critérios especificados nas configurações da regra.
   c. Na lista suspensa **Escopo**, selecione o tipo de arquivo cuja execução será controlada pela regra:
      - **Arquivos executáveis**, se quiser que a regra controle a inicialização de arquivos executáveis.
      - **Pacotes de scripts e MSI**, se quiser que a regra controle a inicialização de scripts e pacotes MSI.
   d. No campo **Usuário ou grupo de usuários**, especifique os usuários que terão permissão ou não para iniciar programas de acordo com o tipo da regra.
      1. No menu de contexto do botão **Procurar**, selecione o método para adicionar usuários confiáveis.

         A janela **Seleção de usuário ou grupo de usuários** é aberta.
      2. Selecione um usuário ou grupo de usuários.
      3. Clique no botão **OK**.
   e. Caso queira obter os valores dos critérios para acionamento de regras listados no bloco **Critério para acionamento da regra** a partir de um arquivo, faça o seguinte:
      1. Clique no botão **Definir critério para acionamento de regras a partir das propriedades do arquivo**.

         A janela **Abrir** padrão do Microsoft Windows é exibida.

2. Selecione o arquivo.

3. Clique no botão **Abrir**.

   O valor dos critérios no arquivo é exibido nos campos no bloco **Critério para acionamento da regra**. O critério para o qual os dados estão disponíveis nas propriedades de arquivo é selecionado por padrão.

f. Na caixa do grupo **Critério para acionamento da regra**, selecione uma ou várias das seguintes opções:

- **Certificado digital**, se quiser que a regra controle a inicialização de programas que usam arquivos assinados com um certificado digital:
  - Marque a caixa de seleção **Usar assunto** se quiser que a regra controle a inicialização de arquivos assinados com um certificado digital somente com o requerente especificado.
  - Marque a caixa de seleção **Usar miniatura** se você quiser que a regra controle a inicialização de arquivos assinados com um certificado digital somente com a impressão digital especificada.
- **Hash SHA256**, se quiser que a regra controle a inicialização de programas que usam os arquivos cuja soma de verificação corresponda àquela especificada.
- **Caminho do arquivo**, se quiser que a regra controle a inicialização de programas que usam os arquivos localizados no caminho especificado.
  - **Linha de comando** se desejar que a regra controle o início de programas iniciados usando os argumentos especificados no campo de linha de comando. O campo é ativado após selecionar a opção **Caminho para o arquivo**. É possível usar os caracteres ? e * como uma máscara ao especificar os argumentos da linha de comando para processos iniciados como um critério.

> O Kaspersky Embedded Systems Security for Windows não reconhece caminhos que contêm barras ("/"). Use a barra invertida ("\") para inserir o caminho corretamente.

> Ao especificar os objetos, você pode usar ? e * caracteres como máscaras de arquivo.

É preciso selecionar ao menos uma opção. Caso contrário, a regra de Controle de Inicialização de Aplicativos não será adicionada.

g. Se deseja adicionar exclusões de regra:

1. Na seção **Exclusões da regra**, clique no botão **Adicionar**.

   A janela **Exclusão da regra** é exibida.

2. No campo **Nome**, digite o nome da exclusão.

3. Especifique as configurações para exclusão dos arquivos de aplicativos da regra de Controle de Inicialização de Aplicativos. Você pode preencher os campos de configurações a partir das propriedades do arquivo clicando no botão **Definir exclusão com base nas propriedades do arquivo**.

   - Certificado digital
   - Usar assunto
   - Usar miniatura

- Hash SHA256
- Caminho do arquivo

4. Clique no botão **OK**.
5. Se necessário, repita os itens (i)-(iv) para incluir exclusões adicionais.

5. Clique no botão **OK** na janela **Configurações de regra**.

A regra criada é exibida na lista na janela **Regras de Controle de Inicialização de Aplicativos**.

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 da KSN de que não são confiáveis. O modo de Permissão padrão pode ser ativado adicionando regras de permissão específicas. Você pode ativar a Permissão padrão apenas para scripts ou para todos os arquivos executáveis.

Para adicionar uma regra de Permissão padrão:

1. Abra a janela **Regras de Controle de Inicialização de Aplicativos**.
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão, selecione **Adicionar uma regra**.
   A janela **Configurações de regra** é exibida.
4. No campo **Nome**, digite o nome da regra.
5. Na lista suspensa **Tipo**, selecione o tipo de regra **Permissão**.
6. Na lista suspensa **Escopo**, selecione o tipo de arquivo cuja execução será controlada pela regra:
   - **Arquivos executáveis**, se quiser que a regra controle a inicialização de arquivos executáveis.
   - **Pacotes de scripts e MSI**, se quiser que a regra controle a inicialização de scripts e pacotes MSI.
7. No grupo **Critério para acionamento da regra**, selecione a opção **Caminho do arquivo**.
8. Insira a seguinte máscara: `?:\`
9. Clique no botão **Configurações de regra** na janela **OK**.

O Kaspersky Embedded Systems Security for Windows aplicará o modo de Permissão padrão.

Criação de regras de permissão a partir de eventos da tarefa de Controle de Inicialização de Aplicativos

Para criar um arquivo de configuração contendo regras de permissão geradas a partir de eventos da tarefa de Controle de Inicialização de Aplicativos:

1. Inicie a tarefa de Controle de Inicialização de Aplicativos no modo **Somente estatísticas** para registrar as informações sobre todas as inicializações de aplicativos em um dispositivo protegido no log de tarefas.

2. Após a conclusão da tarefa no modo **Somente estatísticas**, abra o log de tarefas ao clicar no botão **Abrir log de tarefas** no bloco **Gerenciamento** do painel de detalhes do nó **Controle de Inicialização de Aplicativos**.

3. Na janela **Logs**, clique em **Gerar regras com base em eventos**.

   O Kaspersky Embedded Systems Security for Windows gerará um arquivo de configuração XML contendo a lista de regras com base em eventos da tarefa de Controle de Inicialização de Aplicativos no modo **Somente estatísticas**. Você pode aplicar esta lista de regras na tarefa de Controle de Inicialização de Aplicativos.

Antes de aplicar a lista de regras gerada a partir dos eventos registrados d tarefa, recomendamos que você analise e processe a lista manualmente para certificar-se de que a inicialização de arquivos críticos (por exemplo, arquivos de sistema) seja permitida pelas regras especificadas.

Todos os eventos de tarefa são registrados no log de tarefas independentemente do modo da tarefa. Você pode gerar um arquivo de configuração com uma lista de regras baseada no log criado enquanto a tarefa está sendo executada no modo **Ativa**. Este cenário não é recomendado, exceto em casos urgentes, porque uma lista final de regras deve ser gerada antes que a tarefa seja executada no modo **Ativa** para que seja eficiente.

Exportação de regras do Controle de Inicialização de Aplicativos

Para exportar as regras do Controle de Inicialização de Aplicativos para um arquivo de configuração:

1. Abra a janela **Regras de Controle de Inicialização de Aplicativos**.

2. Clique no botão **Exportar para um arquivo**.

   A janela padrão do Microsoft Windows é exibida.

3. Na janela exibida, especifique o arquivo ao qual deseja exportar as regras. Se nenhum arquivo existir, ele será criado. Se um arquivo com o nome especificado já existir, o seu conteúdo será sobrescrito após a exportação das regras.

4. Clique no botão **Salvar**.

   As configurações de regra serão exportadas para o arquivo especificado.

Importação de regras de Controle de Inicialização de Aplicativos de um arquivo XML

Para importar as regras de Controle de Inicialização de Aplicativos:

1. Abra a janela **Regras de Controle de Inicialização de Aplicativos**.

2. Clique no botão **Adicionar**.

3. No menu de contexto do botão, selecione **Importar regras do arquivo XML**.

4. Especifique o método para adicionar as regras importadas. Para fazer isso, selecione uma das opções do menu de contexto do botão **Importar regras do arquivo XML**:

- **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
- **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas.
- **Mesclar com as regras existentes**, se quiser adicionar as regras importadas à lista de 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 **Abrir** padrão do Microsoft Windows é exibida.

5. Na janela **Abrir**, selecione o arquivo XML que contém as regras de Controle de Inicialização de Aplicativos.
6. Clique no botão **Abrir**.

As regras importadas serão exibidas na lista da janela **Regras de Controle de Inicialização de Aplicativos**.

Removendo regras de Controle de Inicialização de Aplicativos

Para remover as regras de Controle de Inicialização de Aplicativos:

1. Abra a janela **Regras de Controle de Inicialização de Aplicativos**.
2. Na lista, selecione uma ou mais regras que você deseja excluir.
3. Clique no botão **Remover selecionado**.
4. Clique no botão **Salvar**.

As regras de Controle de Inicialização de Aplicativos selecionados são excluídas.

Configuração de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

Para definir as configurações da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Abra a janela **Configurações de tarefa** da tarefa do **Gerador de Regras de Controle de Inicialização de Aplicativos**.
2. Defina as seguintes configurações:
   - Na guia **Geral**:
     - Especifique um **Prefixo para nome de regras**.
     - Configuração do escopo de uso das regras de permissão.
   - Na guia **Ações**, especifique as ações que devem ser executadas pelo Kaspersky Embedded Systems Security for Windows.
   - Nas guias **Agendamento** e **Avançado**, configure a programação de inicialização da tarefa.

- Na guia **Executar como**, defina as configurações de inicialização da tarefa com permissão de conta.

3. Clique em **OK** na janela **Configurações de tarefa**.

O Kaspersky Embedded Systems Security for Windows aplica imediatamente as novas configurações à tarefa em execução. Informações sobre data e hora quando as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação.

Restrição do escopo de uso da tarefa

Para restringir o escopo da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Abra a janela **Configurações de tarefa** da tarefa do **Gerador de Regras de Controle de Inicialização de Aplicativos**.

2. Selecione como criar as regras de permissão:

   - **Criar regras de permissão com base nos aplicativos em execução**.

   - **Criar regras de permissão para aplicativos das pastas**.

3. Clique em **OK** na janela **Configurações de tarefa**.

As configurações especificadas são salvas.

Ações a serem executadas durante a geração automática de regras

Para configurar as ações do Kaspersky Embedded Systems Security for Windows durante a execução e após a conclusão da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Abra a janela **Configurações de tarefa** da tarefa do **Gerador de Regras de Controle de Inicialização de Aplicativos**.

2. Abra a guia **Opções**.

3. No bloco **Ao gerar regras de permissão**, defina as seguintes configurações:

   - **Usar certificado digital**

   - **Usar assunto e miniatura do certificado digital**

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

     - **Hash SHA256**. O valor da soma de verificação do arquivo usado para gerar a regra é estabelecido como o critério para acionamento da regra 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 da regra de permissão de Controle de Inicialização de Aplicativos. O aplicativo agora permitirá a inicialização de programas usando arquivos localizados nas pastas especificadas na tabela **Criar regras de permissão para aplicativos das pastas** na seção **Configurações**.

- Usar hash SHA256.
- Gerar regras para usuário ou grupo de usuários.

4. No bloco **Após a conclusão da tarefa**, defina as seguintes configurações:
   - Adicionar regras de permissão à lista de regras de Controle de Inicialização de Aplicativos.
   - Princípio da adição.
   - **Exportar regras de permissão para o arquivo**.
   - Adicionar os detalhes do dispositivo protegido ao nome do arquivo.
5. Clique em **OK** na janela **Configurações de tarefa**.

As configurações especificadas são salvas.

Ações a serem executadas após a conclusão da geração automática de regras

Para configurar as ações a serem executadas pelo Kaspersky Embedded Systems Security for Windows após a execução da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Abra a janela Configurações de tarefa da tarefa do **Gerador de Regras de Controle de Inicialização de Aplicativos**.
2. Abra a guia **Opções**.
3. No bloco **Após a conclusão da tarefa**, defina as seguintes configurações:
   - Adicionar regras de permissão à lista de regras de Controle de Inicialização de Aplicativos.
   - Princípio da adição.
   - **Exportar regras de permissão para o arquivo**.
   - Adicionar os detalhes do dispositivo protegido ao nome do arquivo.
4. Clique em **OK** na janela **Configurações de tarefa**.

As configurações especificadas são salvas.

Gerenciamento do Controle de Inicialização de Aplicativos por meio do Plug-in da Web

Para configurar tarefas de Controle de Inicialização de Aplicativos por meio do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.

3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.

4. Selecione a seção **Controle de atividades locais**.

5. Clique no botão **Configurações** na subseção **Controle de Inicialização de Aplicativos**.

6. Defina as configurações descritas na tabela a seguir.

Configurações da tarefa de Controle de Inicialização de Aplicativos

Configuração	Descrição
Modo da tarefa.	Nessa lista suspensa, é possível selecionar o modo da tarefa de Controle de Inicialização de Aplicativos: • **Ativa**. O Kaspersky Embedded Systems Security for Windows usa as regras especificadas para controlar a inicialização de qualquer aplicativo. • **Somente estatísticas**. O Kaspersky Embedded Systems Security for Windows não usa regras de Controle de Inicialização de Aplicativos. Ele registra apenas as informações sobre a inicialização de aplicativos no log de tarefas. Todos os aplicativos podem ser inicializados. Você pode usar esse modo para gerar uma lista de regras de Controle de Inicialização de Aplicativos com base nas informações sobre inicializações negadas registradas no log de tarefas. Por padrão, a tarefa de Controle de Inicialização de Aplicativos é executada no modo **Somente estatísticas**.
Repetir ação da primeira inicialização de arquivo em todas as inicializações subsequentes do arquivo	A caixa de seleção ativa ou desativa o controle de inicialização para a segunda tentativa e todas as tentativas subsequentes de inicialização de aplicativos com base nas informações de eventos armazenadas em cache. Caso a caixa de seleção esteja marcada, o Kaspersky Embedded Systems Security for Windows permitirá ou negará uma inicialização subsequente do aplicativo de acordo com a conclusão da tarefa referente à primeira inicialização do aplicativo. Por exemplo, se a primeira inicialização de aplicativo foi permitida pelas regras, as informações sobre essa decisão serão armazenadas em cache e a segunda e todas as inicializações subsequentes também serão permitidas, sem qualquer verificação adicional. Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security for Windows analisará o aplicativo a cada tentativa de inicialização. Por padrão, a caixa de seleção fica desmarcada.
Negar a inicialização de interpretadores de comando sem um comando a executar	Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows negará a inicialização de interpretadores da linha de comando, mesmo que a inicialização de interpretadores seja permitida. Um interpretador da linha de comando só pode ser inicializado sem um comando caso ambas as condições a seguir sejam atendidas: • A inicialização do interpretador da linha de comando é permitida. • O comando a ser executado é permitido. Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security for Windows só considerará as regras de permissão ao inicializar o interpretador da linha de comando. A inicialização será negada se nenhuma regra de permissão for aplicável ou se o processo executável não for considerado confiável pela KSN. Se uma regra de permissão for aplicável ou se o processo for considerado confiável pela KSN, um interpretador da linha de comando pode ser inicializado com ou sem um comando a ser executado.

	O Kaspersky Embedded Systems Security for Windows reconhece os seguintes interpretadores da linha de comando: • cmd.exe • powershell.exe • python.exe • perl.exe Por padrão, a caixa de seleção fica desmarcada.
Aplicar regras a arquivos executáveis	A caixa de seleção ativa ou desativa o controle de inicialização de arquivos executáveis. Se esta caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows permitirá ou bloqueará a inicialização de arquivos executáveis usando as regras especificas cujas definições especificam **Arquivos executáveis** como escopo. Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows não controlará a inicialização de arquivos executáveis usando as regras especificas. A inicialização de arquivos executáveis será permitida. A caixa de seleção é marcada por padrão.
Monitorar o carregamento de módulos DLL	A caixa de seleção ativa ou desativa o controle de carregamento de módulos DLL. Se esta caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows permitirá ou bloqueará o carregamento de módulos DLL usando as regras especificas cujas definições especificam **Arquivos executáveis** como escopo. Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows não controlará o carregamento de módulos DLL usando as regras especificas. O carregamento de módulos DLL será permitido. A caixa de seleção estará ativa se a caixa se seleção **Aplicar regras a arquivos executáveis** estiver marcada. A caixa de seleção é marcada por padrão.
Aplicar regras a scripts e pacotes MSI	A caixa de seleção ativa ou desativa a inicialização de scripts e pacotes MSI. Caso essa caixa de seleção esteja marcada, o Kaspersky Embedded Systems Security for Windows permitirá ou bloqueará a inicialização de scripts e pacotes MSI usando as regras especificas cujas definições especificam **Scripts e pacotes MSI** como escopo. Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows não controlará a inicialização de scripts e pacotes MSI usando regras especificas. A inicialização de scripts e pacotes MSI é permitida. A caixa de seleção é marcada por padrão.
Negar aplicativos não confiáveis pela KSN	A caixa de seleção ativa ou desativa o Controle de Inicialização de Aplicativos de acordo com a reputação do aplicativo na KSN. Se essa caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows bloqueará a execução de qualquer aplicativo que não for considerado confiável pela KSN. As regras de permissão de Controle de Inicialização de Aplicativos que se aplicam a aplicativos não confiáveis pela KSN não serão acionadas. A seleção da caixa fornece proteção adicional contra malware. Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows não considerará a reputação de aplicativos não confiáveis na KSN e permitirá ou bloqueará a inicialização de acordo com as regras que se aplicam a esses programas.

	Por padrão, a caixa de seleção fica desmarcada.
Permitir aplicativos confiáveis pela KSN	A caixa de seleção ativa ou desativa o Controle de Inicialização de Aplicativos de acordo com a reputação do aplicativo na KSN. Se esta caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows permitirá a execução de aplicativos considerados confiáveis pela KSN. Regras de controle de negação de inicialização de aplicativos aplicáveis aos aplicativos considerados como confiáveis pela KSN têm prioridade mais alta: caso um aplicativo seja considerado confiável pelos serviços da KSN, a inicialização desse aplicativo será bloqueada. Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security for Windows não considerará a reputação de aplicativos considerados confiáveis pela KSN e permitirá ou negará a inicialização conforme as regras que se aplicam a esses aplicativos. Por padrão, a caixa de seleção fica desmarcada.
Usuários e/ou grupos de usuários com permissão para executar aplicativos confiáveis pela KSN	Caso a caixa de seleção **Permitir aplicativos confiáveis pela KSN** estiver marcada, aqui é possível especificar os usuários e grupos de usuários com permissão para iniciar os aplicativos confiáveis pela KSN. Por padrão, os seguintes usuários são especificados: **Everyone** e **NT AUTHORITY\SYSTEM**.
Regras	Configure as regras de permissão ou negação para a tarefa de Controle de Inicialização de Aplicativos.
Controle de distribuição de software	Você pode adicionar pacotes de distribuição confiáveis.
Gerenciamento da tarefa	É possível definir configurações para a inicialização programada da tarefa.

Controle de Dispositivos

Esta seção contém informações sobre a tarefa Controle de Dispositivos e como configurá-la.

Sobre a tarefa de Controle de dispositivos

O Kaspersky Embedded Systems Security for Windows controla o registro e o uso de dispositivos externos e unidades de CD/DVD para proteger o dispositivo protegido contra ameaças de segurança que podem ocorrer durante a troca de arquivos com pendrives ou outros tipos de dispositivos externos conectados via USB.

O Kaspersky Embedded Systems Security for Windows controla as seguintes conexões de dispositivos externos USB:

- Pendrive USB, inclusive aqueles compatíveis com UAS
- Unidades de CD/DVD-ROM
- Unidades de disquete conectadas por USB
- Adaptadores de rede conectados por USB
- Dispositivos móveis MTP conectados por USB

O Kaspersky Embedded Systems Security for Windows informará 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 for iniciada, o Kaspersky Embedded Systems Security for Windows verificará e listará 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 dispositivo 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 dispositivo externos conectados:

- *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 no escopo de uso de nenhuma regra de permissão.

Você pode criar regras de permissão para dispositivos externos para permitir a troca de dados usando a tarefa do Gerador de Regras de Controle de Dispositivos. Também é possível expandir o escopo de uso das regras de permissão existentes. Você não pode criar regras de permissão manualmente.

O Kaspersky Embedded Systems Security for Windows identifica os dispositivos externos registrados pelo sistema usando o valor de 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 propriedades Windows e automaticamente determinado pelo Kaspersky Embedded Systems Security for Windows quando as regras de permissão são criadas.

A tarefa de Controle de Dispositivos pode operar em dois modos:

- **Ativa**. O Kaspersky Embedded Systems Security for Windows aplica regras para controlar a conexão de pendrives e outros dispositivos externos e permite ou bloqueia o uso de todos os dispositivos de acordo com o princípio de 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.

  Caso um dispositivo externo considerado não confiável seja conectado a um dispositivo 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 dispositivo protegido. Caso contrário, o princípio de Negação Padrão não será aplicado ao dispositivo.

- **Somente estatísticas**. O Kaspersky Embedded Systems Security for Windows não controla a conexão de pendrives e outros dispositivos externos, só registra em log as informações sobre a conexão e o registro de dispositivos externos em um dispositivo 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.

  É possível aplicar esse modo de geração de regras com base nas informações de bloqueio de dispositivos registradas em log durante a execução da tarefa.

Sobre as regras de Controle de dispositivos

O Kaspersky Embedded Systems Security for Windows não se aplica a regras de permissão para dispositivos móveis conectados ao MTP.

As regras são geradas exclusivamente para cada dispositivo que está conectado atualmente ou foi alguma vez conectado a um dispositivo protegido se as informações sobre este dispositivo estiverem armazenadas no Registro do sistema.

Para gerar as regras de permissão do Controle de Dispositivos:

- Aplicar a tarefa do Gerador de Regras de Controle de Dispositivos.
- Executar a tarefa de Controle de Dispositivos no modo Somente estatísticas.
- Aplicar informações de sistema sobre dispositivos previamente conectados.
- Expandir o escopo de uso das regras já especificadas.

O número máximo de regras de Controle de Dispositivos suportado pelo Kaspersky Embedded Systems Security for Windows é 3072.

As regras de Controle de dispositivos estão descritas abaixo.

Tipo de regra

O tipo de regra é sempre *permissão*. Por padrão, a tarefa de Controle de Dispositivos bloqueia todos os pendrives e outras conexões de dispositivos externos se esses dispositivos não estiverem incluídos em algum escopo de uso da regra de permissão.

Critério para acionamento e escopo de uso da regra

As regras de Controle de Dispositivos identificam pendrives e outros dispositivos externos com base no *Caminho da instância do dispositivo*. O caminho da instância do dispositivo é um critério único atribuído a um dispositivo pelo sistema quando o dispositivo for conectado e registrado como um Dispositivo externo ou uma unidade de CD/DVD (por exemplo, IDE ou SCSI).

O Kaspersky Embedded Systems Security for Windows controla a conexão das unidades de CD/DVD externas independentemente do barramento usado para a conexão. Ao conectar esse dispositivo via USB, o sistema operacional registra dois valores de caminho para a instância do dispositivo: para o dispositivo externo e para a unidade de CD/DVD (por exemplo, IDE ou SCSI). Para conectar esses dispositivos corretamente, as regras de permissão para cada valor de caminho para instância devem ser definidas.

O Kaspersky Embedded Systems Security for Windows define automaticamente o caminho da instância do dispositivo e analisa o valor obtido nos seguintes elementos:

- Fabricante (VID) do dispositivo
- Tipo de controlador (PID) do dispositivo
- Número de série do dispositivo

Você não pode definir manualmente o caminho da instância do dispositivo. Os critérios para acionamento da regra de permissão definem o escopo de uso da regra. Por padrão, o escopo de uso de uma regra de permissão recém-criada inclui o dispositivo inicial cujas propriedades o Kaspersky Embedded Systems Security for Windows usou para gerar a regra. Você pode configurar os valores nas configurações da regra criada usando uma máscara para expandir o escopo de uso da regra.

Valores iniciais de dispositivo

Propriedades de dispositivo que o Kaspersky Embedded Systems Security for Windows usou para permitir a geração de regras e que são exibidas no Gerente de Dispositivos do Windows para cada dispositivo conectado.

Os valores de dispositivo iniciais contêm as seguintes informações:

- **Caminho da instância do dispositivo**. De acordo com essa propriedade, o Kaspersky Embedded Systems Security for Windows define os critérios para acionamento de regras e preenche os seguintes campos: **Fabricante (VID)**, **Tipo de controlador (PID)** e **Número de série** no bloco **Escopo de uso da regra** da janela **Propriedades da regra**.
- **Nome amigável**. O nome claro de dispositivo que é estabelecido nas propriedades de dispositivo por seu fabricante.

O Kaspersky Embedded Systems Security for Windows define automaticamente valores de dispositivo iniciais quando a regra é gerada. Mais tarde você pode usar estes valores para reconhecer o dispositivo que foi usado como base para a geração de regra. Os valores de dispositivo iniciais não estão disponíveis para edição.

Descrição

É possível adicionar informações adicionais para cada regra de Controle de Dispositivos criada no campo **Descrição**, por exemplo, será possível anotar o nome do pendrive conectado ou definir seu proprietário. O comentário é exibido em um gráfico correspondente no campo **Regras de Controle de Dispositivos**.

A descrição e os valores iniciais de dispositivo não são permitidos para o acionamento de regra e são prescritos somente para simplificar uma identificação de dispositivo pelo usuário.

Sobre o Gerador de Regras de Controle de Dispositivos

Você pode importar regras de permissão de controle de dispositivos dos arquivos XML que foram automaticamente gerados durante a execução das tarefas de Controle de dispositivos ou Gerador de Regras de Controle de Dispositivos.

Por padrão, o Kaspersky Embedded Systems Security for Windows bloqueia as conexões de qualquer pendrive e outros dispositivos externos caso eles não estejam incluídos no escopo de uso das regras de controle de dispositivos especificadas.

Finalidades e cenários para gerar regras de controle de dispositivos

Cenário de geração de regra	Destino
A tarefa do Gerador de Regras de Controle de Dispositivos	• Adiciona regras de permissão para dispositivos confiáveis conectados antes da primeira inicialização da tarefa de Controle de dispositivos. • Gere uma lista de regras para dispositivos confiáveis na rede de dispositivos protegidos.
Geração de regras baseada em dados do sistema	Adicione regras de permissão para um ou vários dispositivos externos cujos dados foram armazenados no sistema.
Geração de regras com base em dados sobre os dispositivos conectados no momento	Renove uma lista de regras já especificada quando é necessário confiar em uma pequena quantidade de novos dispositivos de armazenamento em massa.
A tarefa de Controle de Dispositivos no modo **Somente estatísticas**	Gerar regras de permissão para um grande número de dispositivos confiáveis.

O uso da tarefa do Gerador de Regras de Controle de Dispositivos

O arquivo XML, gerado após a conclusão da tarefa do Gerador de Regras de Controle de Dispositivos, contém regras de permissão para aqueles pendrives e outros dispositivos externos cujos dados foram armazenados em um registro do sistema.

Use esse cenário durante o processo de geração de regras para considerar todos os dispositivos externos que já foram conectados alguma vez e que estão registrados pelos sistemas em todos os dispositivos protegidos da rede ou para considerar apenas dados sobre dispositivos conectados a todos os dispositivos protegidos da rede atualmente. A tarefa também permite todos os dispositivos externos conectados no momento da execução da tarefa. Após a conclusão de tarefa de grupo o Kaspersky Embedded Systems Security for Windows gera listas de regras de permissão para todos os dispositivos externos registrados na rede e salva estas listas em um arquivo XML em uma pasta especificada. Em seguida, você pode importar manualmente regras geradas nas configurações da tarefa de Controle de dispositivos. Diferentemente de uma tarefa em um dispositivo protegido, a política não permite configurar a adição automática das regras criadas à lista de regras de Controle de Dispositivos quando a tarefa de grupo do Gerador de Regras de Controle de Dispositivos é concluída.

Este cenário é recomendado para gerar a lista de regras de permissão antes do primeiro início da tarefa de Controle de dispositivos, para que as regras de permissão geradas abranjam todos os dispositivos externos confiáveis que são usados em um dispositivo protegido.

Uso de dados do sistema sobre todos os dispositivos conectados

Durante a execução da tarefa, o Kaspersky Embedded Systems Security for Windows recebe dados do sistema sobre todos os dispositivos externos que foram alguma vez conectados ou que estão atualmente conectados a um dispositivo protegido e exibe os dispositivos detectados na lista da janela **Gerar regras com base nas informações do sistema**.

Para cada dispositivo detectado o Kaspersky Embedded Systems Security for Windows analisa os valores do fabricante (VID), tipo de controlador (PID), nome amigável, número de série e caminho da instância do dispositivo. Você pode gerar regras de permissão para qualquer dispositivo externo cujos dados foram armazenados no sistema e adicionar diretamente regras criadas recentemente à lista das regras de controle de dispositivos.

> De acordo com este cenário, o Kaspersky Embedded Systems Security for Windows gerará regras de permissão para dispositivos externos que já foram conectados alguma vez ou estão atualmente conectados a um dispositivo protegido com o Kaspersky Security Center instalado.

Este cenário é recomendado para renovar uma lista de regras já especificada quando é necessário confiar em uma pequena quantidade de novos dispositivos externos.

Uso de dados sobre os dispositivos conectados no momento

Neste cenário, o Kaspersky Embedded Systems Security for Windows gera regras de permissão apenas para dispositivos externos conectados. É possível selecionar um ou mais dispositivos externos para os quais você deseja gerar regras de permissão.

Uso da tarefa de Controle de Dispositivos no modo Somente estatísticas

O arquivo XML recebido após a conclusão da tarefa de Controle de Dispositivos no modo **Somente estatísticas** é gerado com base no log de tarefas.

Enquanto a tarefa estiver em execução, o Kaspersky Embedded Systems Security for Windows registra em log as informações sobre todas as conexões de pendrives e outros dispositivos externos em um dispositivo protegido. Você pode gerar regras de permissão baseadas em eventos de tarefa e exportá-las a um arquivo XML. Antes de iniciar a tarefa no modo **Somente estatísticas**, recomenda-se configurar o período de execução da tarefa para que durante este tempo especificado sejam realizadas todas as conexões possíveis de dispositivos externos a um dispositivo protegido.

Este cenário é recomendado para renovar uma lista de regras já gerada se isso for necessário para permitir uma quantidade grande de novos dispositivos externos.

Se a geração de lista de regra segundo este cenário for executada em uma máquina modelo, você pode aplicar uma lista de regras de permissão gerada ao configurar a tarefa de Controle de dispositivos através do Kaspersky Security Center. Dessa maneira será possível permitir o uso de dispositivos externos que estejam conectados a uma máquina modelo em todos os dispositivos protegidos.

Sobre a tarefa do Gerador de Regras de Controle de Dispositivos

A tarefa do Gerador de Regras de Controle de Dispositivos pode criar automaticamente uma lista de regras de permissão para pendrives e outros dispositivos externos conectados com base em dados do sistema sobre todos os dispositivos externos que já foram alguma vez conectados a um dispositivo protegido.

Depois da conclusão da tarefa, o Kaspersky Embedded Systems Security for Windows cria um arquivo de configuração XML que contém a lista de regras de permissão para todos os dispositivos externos detectados ou adiciona diretamente regras geradas na tarefa de Controle de dispositivos dependendo das configurações do Gerador de Regras de Controle de Dispositivos. O aplicativo permitirá posteriormente dispositivos para os quais as regras de permissão foram geradas automaticamente.

As regras geradas e adicionadas nas regras da tarefa são exibidas na janela **Regras de Controle de Dispositivos**.

Configurações padrão da tarefa de Controle de dispositivos

Por padrão, a tarefa de Controle de dispositivos possui as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Configurações padrão da tarefa de Controle de dispositivos

Configuração	Valor padrão	Descrição
Modo da tarefa.	**Somente estatísticas**	A tarefa registra informações sobre os dispositivos externos que foram bloqueados ou permitidos de acordo com as regras especificadas. Os dispositivos externos não estão realmente bloqueados. É possível selecionar o modo **Ativa** para que a proteção do dispositivo de fato bloqueie o uso de dispositivos externos.
Permitir o uso de todos os dispositivos externos quando a tarefa Controle de Dispositivos não estiver em execução	Não aplicado	O Kaspersky Embedded Systems Security for Windows bloqueia o uso de dispositivos externos, independente do estado da tarefa de Controle de dispositivos. Isso fornece um nível máximo de proteção contra o surgimento de ameaças à segurança do computador quando arquivos são trocados com dispositivos externos. Você pode ajustar a configuração para que o Kaspersky Embedded Systems Security for Windows permita o uso de todos os dispositivos externos quando a tarefa de Controle de dispositivos não for executada.
Programação de inicialização da tarefa	A primeira execução não está programada.	A tarefa de Controle de dispositivos não inicia automaticamente no momento da inicialização do Kaspersky Embedded Systems Security for Windows. Você pode configurar a programação de inicialização da tarefa.

Configurações padrão da tarefa do Gerador de Regras de Controle de Dispositivos

Configuração	Valor padrão	Descrição
Modo da tarefa.	**Considerar dados do sistema de todos os dispositivos externos que já foram conectados**	Modo operacional da tarefa. Você pode selecionar o modo da tarefa **Considerar somente dispositivos externos conectados no momento**.
Ações após a conclusão da tarefa	As regras de permissão são adicionadas à lista das regras de Controle de dispositivos; as novas regras são agregadas às existentes; as regras duplicadas são removidas.	Você pode adicionar regras às regras existentes sem agregá-las e sem apagar as regras duplicadas, ou substituir as regras existentes por regras novas de permissão ou configurar a exportação de regras de permissão para um arquivo.
Programação de inicialização da tarefa	A primeira execução não está programada.	A tarefa do Gerador de Regras de Controle de Dispositivos não inicia automaticamente no momento da inicialização do Kaspersky Embedded Systems Security for Windows. É possível iniciar a tarefa manualmente ou configurar um início programado.

Gerenciamento do Controle de Dispositivos por meio do Plug-in de Administração

Nesta seção, saiba como navegar pela interface do Plug-in de Administração e gerenciar conexões de qualquer dispositivo externo para todos os dispositivos protegidos na rede gerando listas de regras por meio do Kaspersky Security Center para os grupos de dispositivos protegidos.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das configurações de política para a tarefa de Controle de Dispositivos

Para abrir a configuração da tarefa de Controle de Dispositivos por meio da política do Kaspersky Security Center:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Controle de atividades locais**.
6. Clique no botão **Configurações**, na subseção **Controle de dispositivos**.

   A janela **Controle de Dispositivos** será aberta.

7. Configure a política conforme necessário.

Abertura da lista de regras de Controle de Dispositivos

Para abrir a lista de regras de Controle de Dispositivos por meio do Kaspersky Security Center:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Controle de atividades locais**.
6. Clique no botão **Configurações**, na subseção **Controle de dispositivos**.

   A janela **Controle de Dispositivos** será aberta.
7. Na guia **Geral**, clique no botão **Lista de regras**.

   A janela **Regras de Controle de dispositivos** é exibida.
8. Configure a política conforme necessário.

Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Dispositivos

Para inicializar a criação da tarefa do Gerador de Regras de Controle de Dispositivos:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Abra a guia **Tarefas**.
4. Clique no botão **Nova tarefa**.

   A janela **Assistente de Nova Tarefa** será aberta.
5. Selecione a tarefa **Gerador de Regras de Controle de Dispositivos**.
6. Clique no botão **Avançar**.

   A janela **Configurações** é exibida.

Para configurar a tarefa do Gerador de Regras de Controle de Dispositivos:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.

3. Abra a guia **Tarefas**.

4. Clique duas vezes no nome da tarefa na lista de tarefas no Kaspersky Security Center.

   A janela **Propriedades: Gerador de Regras de Controle de Dispositivos** é exibida.

Consulte a seção Configuração da tarefa do Gerador de regras de controle de dispositivos para detalhes sobre a configuração da tarefa.

Configuração da tarefa de Controle de Dispositivos

Para definir as configurações da tarefa de Controle de dispositivos:

1. Abra a janela **Controle de Dispositivos**.

2. Na guia **Geral**, defina as seguintes configurações de tarefa:

   - No bloco **Modo da tarefa**, selecione um dos modos de tarefa:

     - Ativa.

       Caso um dispositivo externo considerado não confiável seja conectado em um dispositivo protegido antes que a tarefa de Controle de Dispositivos seja iniciada no modo Ativa, o dispositivo não será bloqueado pelo aplicativo. Recomendamos que desconecte o dispositivo não confiável manualmente ou reinicie o dispositivo protegido. Caso contrário, o princípio de Negação Padrão não será aplicado ao dispositivo.

     - **Somente estatísticas**.

   - Marque ou desmarque a caixa de seleção **Permitir o uso de todos os dispositivos externos quando a tarefa Controle de Dispositivos não estiver em execução**.

3. Clique no botão **Lista de regras** para editar a lista de regras de Controle de Dispositivos.

4. Caso necessário, configure a programação de inicialização da tarefa na guia **Gerenciamento da tarefa**.

5. Clique no botão **OK** na janela **Controle de Dispositivos**.

O Kaspersky Embedded Systems Security for Windows aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Configurando a tarefa do Gerador de Regras de Controle de Dispositivos

Para configurar a tarefa do Gerador de Regras de Controle de Dispositivos:

1. Abra a janela **Propriedades: Gerador de Regras de Controle de Dispositivos**.

2. 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*.

3. Na seção **Configurações**, é possível definir as seguintes configurações:

   - Selecione o modo de operação: considere dados de sistema sobre todos os dispositivos externos que já estiveram conectados alguma vez ou considere somente os dispositivos externos conectados atualmente.
   - Defina as configurações para arquivos de configuração com listas de regras de permissão que o Kaspersky Embedded Systems Security for Windows cria após a conclusão da tarefa.

4. Configure a programação da tarefa na seção **Agendamento** (é possível configurar uma programação para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).

5. Na seção **Conta**, especifique a conta cujos direitos serão usados para executar a tarefa.

6. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

   Para obter informações detalhadas sobre as definições das configurações nessas seções, consulte a *Ajuda do Kaspersky Security Center*.

7. Clique no botão **OK** na janela **Propriedades: <Nome da tarefa>**.

   As recém-definidas configurações da tarefa de grupo são salvas.

Configuração de regras de Controle de Dispositivos por meio do Kaspersky Security Center

Aprenda como gerar uma lista de regras com base em vários critérios ou crie regras de permissão ou negação manualmente usando a tarefa de Controle de Dispositivos.

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 tarefa de Controle de dispositivos:*

1. Se necessário, conecte um novo dispositivo externo que você deseja definir como confiável a um dispositivo protegido com o Console de Administração do Kaspersky Security Center instalado.

2. Abra a janela **Regras de Controle de dispositivos**.

3. Clique no botão **Adicionar** e, no menu de contexto exibido, selecione a opção **Gerar regras com base nos dados do sistema**.

4. Na lista de dispositivos na janela **Gerar regras com base nas informações do sistema**, selecione um dispositivos.

5. Clique no botão **Adicionar regras para os dispositivos selecionados**.

6. Clique no botão **Salvar** na janela **Regras de Controle de dispositivos**.

A lista de regras na tarefa de Controle de dispositivos será preenchida com novas regras geradas com base em dados do sistema do dispositivo protegido 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 dispositivos conectados** na tarefa de Controle de dispositivos:*

1. Abra a janela **Regras de Controle de dispositivos**.

2. Clique no botão **Adicionar** e, no menu de contexto, selecione **Gerar regras com base nos dispositivos conectados**.

   A janela **Gerar regras com base nas informações do sistema** é exibida.

3. Na lista de dispositivos detectados conectados ao dispositivo protegido, selecione os dispositivos para os quais você deseja gerar as regras de permissão.

4. Clique no botão **Adicionar regras para os dispositivos selecionados**.

5. Clique no botão **Salvar** na janela **Regras de Controle de dispositivos**.

A lista de regras na tarefa de Controle de dispositivos será preenchida com novas regras geradas com base em dados do sistema do dispositivo protegido com o Console de Administração do Kaspersky Security Center instalado.

Gerando regras baseadas no registro do Kaspersky Security Center

*Para especificar as regras de permissão usando a opção **Gerar regras com base nos dispositivos conectados** na tarefa de Controle de Dispositivos:*

1. Abra a janela **Regras de Controle de dispositivos**.

2. Clique no botão **Adicionar** e, no menu de contexto, selecione **Gerar regras com base nos dispositivos conectados**.

   A janela **Gerar regras com base nas informações do sistema** é aberta.

3. Clique em **Atualizar a lista** para obter a lista de dispositivos disponíveis e selecione os dispositivos para os quais deseja gerar regras de permissão. Além disso, é possível especificar o **Nome amigável** no campo de **Pesquisa** para filtrar os dispositivos e acelerar a seleção.

4. Clique no botão **Adicionar regras para os dispositivos selecionados**.

5. Clique no botão **Salvar** na janela **Regras de Controle de dispositivos**.

A lista de regras na tarefa de Controle de Dispositivos será preenchida com novas regras geradas de acordo com o registro do Kaspersky Security Center.

Visualizando propriedades das regras do Controle de Dispositivos

Para visualizar as propriedades das regras de **Controle de Dispositivos**:

1. Abra a janela **Controle de Dispositivos**.
2. Na guia **Geral**, clique no botão **Lista de regras** e clique duas vezes na regra selecionada.

   A janela **Propriedades da regra** é exibida.

Propriedades das regras de Controle de Dispositivos

Propriedade	Descrição
Aplicar regra	Use essa opção para ativar ou desativar o aplicativo de regra.
Fabricante (VID)	É possível especificar o VID completo do fornecedor do dispositivo ou usar o caractere * como uma máscara. O caractere * é usado para identificar qualquer fabricante. Caso a caixa de seleção Usar máscara seja marcada para o fabricante (VID), os dados dos campos com a caixa marcada serão substituídos por um * e não serão considerados quando a regra for aplicada.
Tipo de controlador (PID)	É possível especificar o PID completo do controlador ou usar o caractere * como uma máscara. O caractere * é usado para indicar qualquer tipo de controlador. Caso a caixa de seleção Usar máscara esteja marcada no campo Tipo de controlador (PID), os dados dos campos com a caixa marcada serão substituídos por um * e não serão considerados quando a regra for aplicada.
Número de série	É possível especificar o número de série completo do dispositivo ou usar os caracteres * ou ? como uma máscara. O caractere * denota qualquer sequência de caracteres, inclusive uma sequência vazia. O ? caractere denota um único caractere em uma sequência. Caso a caixa de seleção Usar máscara esteja marcada para o campo Número de série, os dados do campo com a caixa selecionada serão substituídos por um caractere * e não serão considerados quando a regra for aplicada. Caso tenha selecionado a opção **Usar uma máscara**, mas não inserir nenhum caractere no campo **Número de série**, então salve as configurações e feche a janela, o aplicativo aplica * como uma máscara para a propriedade **Número de série** e não considera o campo quando a regra é aplicada.
Caminho da instância do dispositivo	Identificador do dispositivo conectado. Não é possível modificar a propriedade. O campo é apenas informativo. O aplicativo não aplica o campo para controle de dispositivos.
Nome amigável	Nome do dispositivo definido pelo fabricante. Não é possível modificar a propriedade. O campo é apenas informativo. O aplicativo não aplica o campo para controle de dispositivos.
Usuário ou grupo de usuários	Existem muitas maneiras de especificar uma conta de usuário ou um grupo de usuários com acesso aos dispositivos USB selecionados. • usando o Active Directory Domain Services • usando a lista de usuários e grupos de usuários do Servidor de Administração • adicionando manualmente.

	O sistema operacional exibe todos os dispositivos USB conectados. É possível acessar apenas as unidades USB para as quais houver os respectivos direitos de acesso.
Descrição	A descrição do dispositivo padrão. Caso necessário, especifique as informações adicionais sobre a regra no campo Descrição. Por exemplo, especifique os dispositivos afetados pela regra.

Importação de regras a partir do relatório do Kaspersky Security Center sobre dispositivos bloqueados

É possível importar os dados sobre as conexões de dispositivos bloqueados do relatório gerado no Kaspersky Security Center após a conclusão da tarefa de Controle de Dispositivos no modo **Somente estatísticas** e usar esses 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.

Para especificar regras de permissão para a conexão de dispositivos para um grupo de dispositivos protegidos com base no relatório do Kaspersky Security Center sobre dispositivos bloqueados:

1. Nas propriedades da política, na seção **Notificação de evento**, certifique-se de que:

   - Para o nível de importância **Eventos Críticos**, o período de armazenamento do log de tarefas para o evento Dispositivo externo não confiável detectado e restrito excede o tempo planejado de operação no modo **Somente estatísticas** (o valor padrão é de 30 dias).

   - Para o nível de importância **Aviso**, o período de armazenamento do log de tarefas para o evento Somente estatísticas: dispositivo externo não confiável detectado excede o tempo planejado de operação da tarefa no modo **Somente estatísticas** (o valor padrão é de 30 dias).

     Quando o período especificado para armazenamento dos eventos for excedido, as informações sobre eventos registrados serão excluídas e não serão refletidas no relatório. Antes de executar a tarefa de Controle de Dispositivos no modo **Somente estatísticas**, verifique e confirme se o tempo de execução da tarefa não excede o tempo de armazenamento configurado para os eventos especificados.

2. Inicie a tarefa de Controle de Dispositivos no modo **Somente estatísticas**.

   a. Na área de trabalho do node **Servidor de Administração** no Kaspersky Security Center, selecione a guia **Eventos**.

   b. Clique no botão **Criar seleção** e crie uma seleção de eventos de acordo com o critério Dispositivo externo não confiável detectado e restrito. Visualize as conexões dos dispositivos bloqueados pela tarefa Controle de Dispositivos.

   c. No painel de resultados da seleção, clique no link **Exportar eventos para arquivo** para salvar o relatório de conexões restritas 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.

3. Importar dados sobre conexões de dispositivos restritos na tarefa de Controle de dispositivos:

   a. Abra a janela **Regras de Controle de dispositivos**.

   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:

- **Mesclar com as regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas não são duplicadas. Se pelo menos uma configuração de regra for exclusiva, a regra será adicionada.
- **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
  - **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas.

   a. Na janela padrão do Microsoft Windows exibida, selecione o arquivo TXT ao qual os eventos do relatório sobre dispositivos restringidos foram exportados.

   b. Clique no botão **Salvar** na janela **Regras de Controle de dispositivos**.

4. Clique no botão **OK** na janela **Controle de Dispositivos**.

As regras criadas com base no relatório do Kaspersky Security Center sobre dispositivos restringidos são adicionadas à lista de regras de Controle de dispositivos.

Criação de regras usando a tarefa do Gerador de Regras de Controle de Dispositivos

Para especificar regras de permissão de controle de dispositivos para um grupo de dispositivos protegidos usando a tarefa do Gerador de Regras de Controle de Dispositivos:

1. Abra a janela **Configurações** no Assistente para Novas Tarefas.

2. Defina as seguintes configurações:

- No bloco **Modo**:
  - **Considerar dados do sistema de todos os dispositivos externos que já foram conectados**
  - **Considerar somente dispositivos externos conectados no momento**
- No bloco **Após a conclusão da tarefa**:
  - Adicionar regras de permissão à lista de regras de Controle de dispositivos.
  - **Princípio da adição**.
  - **Exportar regras de permissão para o arquivo**.
  - **Adicionar os detalhes do dispositivo protegido ao nome do arquivo**.

3. Clique no botão **Avançar**.
4. Na janela **Agendamento**, especifique as configurações da programação de inicialização da tarefa.
5. Clique no botão **Avançar**.
6. Na janela **Seleção de uma conta para a execução da tarefa**, especifique a conta que deseja usar.
7. Clique no botão **Avançar**.
8. Especifique um nome de tarefa.
9. Clique no botão **Avançar**.

   O nome da tarefa não deve ter mais de 100 caracteres e não pode conter os seguintes símbolos: " * < > & \ : |

   A janela **Concluir a criação da tarefa** é exibida.
10. Você também pode executar a tarefa após a finalização do Assistente marcando a caixa de seleção **Executar a tarefa após a finalização do Assistente**.
11. Clique em **Concluir** para concluir a criação da tarefa.
12. Na guia **Tarefas** na área de trabalho do grupo de dispositivos protegidos que estão sendo configurados, na lista de tarefas de grupo, selecione o Gerador de Regras de Controle de Dispositivos criado.
13. Clique no botão **Iniciar** para iniciar a tarefa.

    Quando a tarefa for concluída, as listas de regras de permissão geradas automaticamente serão salvas em arquivos XML em uma pasta compartilhada.

    Antes de usar a política de Controle de Dispositivos na rede, certifique-se de que todos os dispositivos protegidos tenham acesso a uma pasta de rede compartilhada. Caso a política da organização não permita o uso de uma pasta compartilhada na rede, é recomendável iniciar a tarefa de Gerador de Regras de Controle de Dispositivos para as regras de controle do dispositivo protegido no grupo de dispositivos protegidos de teste ou em uma máquina modelo.

Adicionar as regras geradas à lista de regras de Controle de Dispositivos

Para adicionar as listas geradas de regras de permissão à tarefa de Controle de dispositivos:

1. Abra a janela **Regras de Controle de dispositivos**.
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão **Adicionar**, selecione a opção **Importar regras do arquivo XML**.
4. Selecione o princípio para adicionar as regras de permissão geradas automaticamente à lista de regras de Controle de dispositivos criadas anteriormente:

- **Mesclar com as regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas não são duplicadas. Se pelo menos uma configuração de regra for exclusiva, a regra será adicionada.

- **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.

5. **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas. 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.

6. Clique no botão **Abrir**.

   Todas as regras geradas do arquivo XML serão adicionadas à lista de acordo com o princípio selecionado.

7. Clique no botão **Salvar** na janela **Regras de Controle de dispositivos**.

8. Caso queira aplicar as regras de Controle de Dispositivos geradas, selecione o modo de tarefa **Controle de Dispositivos** nas configurações de política de **Ativa**.

Regras de permissão geradas automaticamente com base em dados do sistema em cada dispositivo protegido separado são aplicadas a todos os dispositivos protegidos de rede abrangidos pela política sendo configurada. Nestes dispositivos protegidos, o aplicativo permitirá a conexão somente daqueles dispositivos para os quais as regras de permissão foram criadas.

Gerenciamento do Controle de Dispositivos por meio do Console do Aplicativo

Nesta seção, aprenda a navegar pela interface do Console do Aplicativo e definir as configurações de tarefa em um dispositivo protegido.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das configurações da tarefa de Controle de Dispositivos

Para abrir as configurações da tarefa do Controle de Dispositivos por meio do Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o node **Controle do Computador**.

2. Selecione o nó filho **Controle de Dispositivos**.

3. No painel de detalhes do nó filho **Controle de Dispositivos**, clique no link **Propriedades**.

   A janela **Configurações de tarefa** é aberta.

4. Configure a tarefa conforme necessário.

Abertura da janela de regras de Controle de dispositivos

Para abrir a lista de regras de Controle de Dispositivos por meio do Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o node **Controle do Computador**.
2. Selecione o node secundário **Controle de Dispositivos**.
3. No painel de resultados do node **Controle de Dispositivos**, clique no link **Regras de Controle de Dispositivos**.
   A janela **Regras de Controle de Dispositivos** é exibida.
4. Configure a lista de regras conforme necessário.

Abertura das configurações da tarefa do Gerador de Regras de Controle de Dispositivos

Para configurar a tarefa do Gerador de Regras de Controle de Dispositivos:

1. Na árvore do Console do Aplicativo, expanda o node **Geradores de regras automatizadas**.
2. Selecione o node secundário **Gerador de Regras de Controle de Dispositivos**.
3. No painel de resultados do node secundário **Gerador de Regras de Controle de Dispositivos**, clique no link **Propriedades**.
   A janela **Configurações de tarefa** é aberta.
4. Configure a tarefa conforme necessário.

Definindo as configurações de tarefa de Controle de dispositivos

Para definir as configurações da tarefa de Controle de dispositivos:

1. Abra a janela **Configurações de tarefa**.
2. Na guia **Geral**, defina as seguintes configurações de tarefa:
   - No bloco **Modo da tarefa**, selecione um dos modos de tarefa:
     - Ativa.

     Caso um dispositivo externo considerado não confiável seja conectado em um dispositivo protegido antes que a tarefa de Controle de Dispositivos seja iniciada no modo Ativa, o dispositivo não será bloqueado pelo aplicativo. Recomendamos que desconecte o dispositivo não confiável manualmente ou reinicie o dispositivo protegido. Caso contrário, o princípio de Negação Padrão não será aplicado ao dispositivo.

- **Somente estatísticas**.

- Marque ou desmarque a caixa de seleção **Permitir o uso de todos os dispositivos externos quando a tarefa Controle de Dispositivos não estiver em execução**.

3. Caso necessário, nas guias **Agendamento** e **Avançado**, defina as configurações da programação de inicialização da tarefa.

4. Para editar a lista de regras de controle de dispositivos, clique no link **Regras de Controle de Dispositivos** na parte inferior do painel de resultados do node **Controle de Dispositivos**.

O Kaspersky Embedded Systems Security for Windows aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Configuração de regras de Controle de dispositivos

Aprenda como gerar, importar e exportar uma lista de regras, ou criar manualmente regras de permissão ou de negação utilizando a tarefa de Controle de Dispositivos.

Importando as regras de Controle de dispositivos do arquivo XML

Para importar regras de Controle de Dispositivos:

1. Abra a janela **Regras de Controle de Dispositivos**.

2. Clique no botão **Adicionar**.

3. No menu de contexto do botão, selecione **Importar regras do arquivo XML**.

4. Especifique o método para adicionar as regras importadas. Para fazer isso, selecione uma das opções do menu de contexto do botão **Importar regras do arquivo XML**:

   - **Adicionar às regras existentes**, caso queira adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.

   - **Substituir as regras existentes**, caso queira substituir as regras existentes pelas importadas.

   - **Mesclar com as regras existentes**, caso queira 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 **Abrir** padrão do Microsoft Windows é exibida.

5. Na janela **Abrir**, selecione o arquivo XML que contém as configurações das regras de Controle de dispositivos.

6. Clique no botão **Abrir**.

As regras importadas serão exibidas na lista da janela **Regras de Controle de Dispositivos**.

Preenchendo a lista de regras com base em eventos de tarefa de Controle de dispositivos

Para criar um arquivo de configuração que contenha regras de controle de dispositivos com base nos eventos da tarefa de Controle de dispositivos:

1. Inicie a tarefa de Controle de Dispositivos no modo **Somente estatísticas** para registrar em log todos as conexões de pendrives e outros dispositivos externos em um dispositivo protegido.

2. Após concluir a tarefa no modo **Somente estatísticas**, abra o log de tarefas clicando no botão **Abrir log de tarefas** na seção **Gerenciamento** do node **Controle de Dispositivos** no painel de resultados.

3. Na janela **Logs**, clique em **Gerar regras com base em eventos**.

   O Kaspersky Embedded Systems Security for Windows criará um arquivo de configuração XML que contém a lista de regras gerada com base em eventos de tarefa de Controle de dispositivos no modo **Somente estatísticas**. Você pode aplicar essa lista à tarefa de Controle de Dispositivos.

Antes de aplicar uma lista de regras gerada com base nos eventos de tarefa, recomenda-se analisar e, em seguida, processar manualmente a lista de regras para se certificar de que não haja dispositivos não confiáveis permitidos pelas regras especificadas.

Durante a conversão de um arquivo XML com os eventos de tarefa para uma lista de regras de controle de dispositivos, o aplicativo gera regras de permissão para todos os eventos registrados, inclusive as restrições de dispositivos.

Todos os eventos de tarefa são registrados no log de tarefas independente do modo de tarefa. Você pode criar um arquivo de configuração com uma lista de regras com base nos eventos da tarefa no modo **Ativa**. Este cenário não é recomendado, exceto em casos urgentes, desde que a eficiência da tarefa necessite gerar uma versão de lista de regras final antes que a tarefa seja executada no modo Ativa.

Adicionar uma regra de permissão para um ou vários dispositivos externos

A função do manual que adiciona regras uma por vez não é suportada na tarefa de Controle de dispositivos. No entanto, em casos onde é necessário adicionar regras de um ou vários dispositivos externos novos, é possível usar a opção **Gerar regras com base nos dados do sistema**. Se este cenário for aplicado, o aplicativo utilizará dados do Windows sobre todos os dispositivos externos já conectados e também permite que dispositivos atualmente conectados preencham uma lista de regras de permissão.

Para adicionar uma regra de permissão para um ou mais dispositivos externos que estão conectados atualmente:

1. Abra a janela **Regras de Controle de Dispositivos**.

2. Clique no botão **Adicionar**.

3. No menu de contexto exibido selecione a opção **Gerar regras com base nos dados do sistema**.

4. Na janela exibida, reveja a lista de dispositivos detectados e selecione um dispositivo único ou vários dispositivos nos quais deseja confiar em um dispositivo protegido.

5. Clique no botão **Adicionar regras para os dispositivos selecionados**.

As novas regras serão geradas e adicionadas à lista de regras de controle de dispositivos.

Removendo regras de Controle de dispositivos

Para remover regras de Controle de dispositivos:

1. Abra a janela **Regras de Controle de Dispositivos**.
2. Na lista, selecione uma ou várias regras que deseja excluir.
3. Clique no botão **Remover selecionado**.
4. Clique no botão **Salvar**.

As regras de Controle de dispositivos selecionadas serão removidas.

Exportando regras de Controle de dispositivos

Para exportar as regras de Controle de dispositivos para um arquivo de configuração:

1. Abra a janela **Regras de Controle de Dispositivos**.
2. Clique no botão **Exportar para um arquivo**.

   A janela padrão do Microsoft Windows é exibida.
3. Na janela exibida, especifique o arquivo ao qual deseja exportar as regras. Se nenhum arquivo existir, ele será criado. Se um arquivo com o nome especificado já existir, os seus conteúdos serão reescritos após as regras terem sido exportadas.
4. Clique no botão **Salvar**.

As regras e as suas configurações serão exportadas no arquivo especificado.

Ativando e desativando regras de Controle de dispositivos

É possível ativar e desativar as regras de Controle de Dispositivos criadas sem removê-las.

Para ativar ou desativar uma regra de controle de dispositivos criada:

1. Abra a janela **Regras de Controle de Dispositivos**.
2. Na lista de regras especificadas, abra a janela **Propriedades da regra** clicando duas vezes na regra cujas propriedades você deseja configurar.
3. Na janela exibida, selecione ou desmarque a caixa **Aplicar regra**.
4. Clique no botão **OK**.

O Status de aplicação da regra será salvo e exibido para a regra especificada.

Expandindo o escopo de uso das regras de Controle de dispositivos

Cada regra de controle de dispositivos gerada automaticamente abrange somente um dispositivo externo. É possível expandir manualmente um escopo de uso de regra ao estabelecer a máscara do caminho da instância do dispositivo nas propriedades de qualquer regra de controle de dispositivos especificada.

Usar uma máscara de caminho de instância de dispositivo reduz o número total de regras de controle de dispositivos permitidas e simplifica o processamento de regras. Mas a expansão de um escopo de uso da regra pode levar à redução da eficiência de controle de dispositivos externos.

Para aplicar uma máscara de caminho da instância do dispositivo em propriedades da regra de controle de dispositivos:

1. Abra a janela **Regras de Controle de Dispositivos**.
2. Na janela que se abre, selecione uma regra para usar suas propriedades para o aplicativo de máscara.
3. Abra a janela **Propriedades da regra** clicando duas vezes em uma regra de Controle de dispositivos selecionada.
4. Na janela exibida, execute as seguintes operações:
   - Marque a caixa de seleção **Usar máscara** ao lado do campo **Fabricante (VID)** se desejar que uma regra selecionada permita conexões para todos os dispositivos externos que corresponderem às informações especificadas sobre o fabricante do dispositivo.
   - Marque as caixas de seleção **Usar máscara** ao lado do campo **Tipo de controlador (PID)** se desejar que uma regra selecionada permita conexões para todos os dispositivos externos que corresponderem às informações especificadas sobre o tipo de controlador.
   - Marque a caixa de seleção **Usar máscara** ao lado do campo **Número de série** se quiser que uma regra selecionada permita as conexões para todos os dispositivos externos que corresponderem às informações especificadas sobre o número de série.

   Caso a caixa de seleção **Usar máscara** for marcada em pelo menos um dos campos, os dados dos campos com a caixa selecionada serão substituídos por um * e não serão considerados quando a regra for aplicada.
5. Especifique uma conta de usuário ou um grupo de usuários que têm acesso aos dispositivos USB selecionados. O sistema operacional exibe todos os dispositivos USB conectados. É possível acessar apenas os dispositivos USB para os quais tiver os respectivos direitos de acesso.
6. Caso necessário, especifique as informações adicionais sobre a regra no campo **Usuário ou grupo de usuários**. Por exemplo, especifique os dispositivos afetados pela regra.
7. Clique no botão **OK**.

As propriedades da regra definidas recentemente serão salvas. O escopo de uso da regra será expandido de acordo com uma máscara de caminho da instância do dispositivo especificada.

Configurando a tarefa do Gerador de Regras de Controle de Dispositivos

Para configurar a tarefa do Gerador de Regras de Controle de Dispositivos:

1. Na árvore do Console do Aplicativo, expanda o node **Geradores de regras automatizadas**.
2. Selecione o node secundário **Gerador de Regras de Controle de Dispositivos**.
3. No painel de resultados do node secundário **Propriedades**, clique no link **Gerador de Regras de Controle de Dispositivos**.

   A janela **Configurações de tarefa** é aberta.
4. Na guia **Geral**, selecione o modo da tarefa no bloco **Modo da tarefa**:
   - **Considerar dados do sistema de todos os dispositivos externos que já foram conectados**
   - **Considerar somente dispositivos externos conectados no momento**
5. Na seção **Após a conclusão da tarefa**, especifique as ações que devem ser executadas pelo Kaspersky Embedded Systems Security for Windows após a conclusão da tarefa:
   - Adicionar regras de permissão à lista de regras de Controle de dispositivos.
   - Princípio da adição.
   - Exportar regras de permissão para o arquivo.
   - Adicionar os detalhes do dispositivo protegido ao nome do arquivo.
6. Nas guias **Agendamento** e **Avançado**, configure a programação de inicialização da tarefa.
7. Clique em **OK** na janela **Configurações de tarefa**.

O Kaspersky Embedded Systems Security for Windows aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Gerenciamento do Controle de Dispositivos por meio do Plug-in da Web no Console do Aplicativo

Nessa seção, você aprenderá a navegar pela interface do Plug-in da Web e definir as configurações de tarefa em um dispositivo protegido.

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Controle de atividades locais**.
5. Clique no botão **Configurações**, na subseção **Controle de Dispositivos**.
6. Defina as configurações descritas na tabela a seguir.

Configurações da tarefa de Controle de Dispositivos

Configuração	Descrição
Ativa	O Kaspersky Embedded Systems Security for Windows aplica regras para controlar a conexão de unidades removíveis e outros dispositivos externos e permite ou bloqueia o uso de todos os dispositivos de acordo com o princípio de 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.
Somente estatísticas	O Kaspersky Embedded Systems Security for Windows não controla a conexão de unidades removíveis e outros dispositivos externos, apenas registra em log as informações sobre a conexão e o registro de dispositivos externos em um dispositivo 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.
Permitir o uso de todos os dispositivos externos quando a tarefa Controle de Dispositivos não estiver em execução	A caixa de seleção permite ou bloqueia a utilização de dispositivos externos quando a tarefa de Controle de dispositivos não estiver sendo executada. Caso a caixa de seleção seja marcada e a tarefa de Controle de dispositivos não estiver sendo executada, o Kaspersky Embedded Systems Security for Windows permitirá a utilização de qualquer dispositivo externo em um dispositivo protegido. Caso a caixa de seleção esteja desmarcada, o aplicativo bloqueará a utilização de dispositivos externos não confiáveis em um dispositivo protegido nos seguintes casos: quando a tarefa de Controle de dispositivos não estiver sendo executada ou se o Kaspersky Security Service tiver sido desativado. Essa opção é recomendada para maximizar o nível da proteção contra ameaças de segurança do computador que surgem após a troca de arquivos com dispositivos externos. Por padrão, a caixa de seleção fica desmarcada.
Regras de Controle de Dispositivos	Você pode editar a lista de Regra de Controle de Dispositivos.
Gerenciamento de tarefas	É possível definir configurações para a inicialização programada da tarefa.

Gerenciamento de Firewall

Esta seção contém informações sobre a tarefa Gerenciamento de Firewall e como configurá-la.

Sobre a tarefa de Gerenciamento de Firewall

Se o Firewall do Windows for desativado durante a instalação do Kaspersky Embedded Systems Security for Windows, a tarefa de Gerenciamento de Firewall não será executada após a conclusão da instalação. Caso o Firewall do Windows esteja ativado durante a instalação, a tarefa Gerenciamento de Firewall será executada após a conclusão da instalação.

Se o Firewall do Windows for gerenciado por uma política de grupo do Kaspersky Security Center, a tarefa de Gerenciamento de Firewall não poderá ser iniciada.

A tarefa Gerenciamento de Firewall não filtra o tráfego de rede de forma independente, mas permite gerenciar o Firewall do Windows pela interface gráfica do Kaspersky Embedded Systems Security for Windows.

A tarefa sonda o Firewall do Windows regularmente. Por padrão, o intervalo de pesquisa é definido como um minuto e não pode ser alterado.

Durante a execução da tarefa de Gerenciamento de Firewall, o Kaspersky Embedded Systems Security for Windows executa as ações definidas pelo modo de interação com o Firewall do Windows:

- **Observar o estado do Firewall do Windows**. O aplicativo monitora apenas o status do Firewall do Windows e envia um evento de aviso ao Kaspersky Security Center caso o Firewall do Windows não seja iniciado.
- **Controlar a operação do Firewall do Windows**. O aplicativo controla a operação do Firewall do Windows na medida determinada pelas seguintes funções:
  - Manter o estado do Firewall do Windows

    Esse recurso ativa ou desativa a manutenção do Firewall do Windows no estado **Ativado/Desativado** com o uso da lista suspensa.

    Caso a função esteja ativada, o aplicativo executa as seguintes ações:

    - Faz a sondagem do Firewall do Windows em um intervalo de um minuto.
    - Lê o status do Firewall do Windows.
    - Quando o status for definido como **Ativado**, ativa o Firewall do Windows caso esteja desativado.
    - Quando o status for definido como **Desativado**, desativa o Firewall do Windows caso esteja ativado.

    Esse recurso não pode ser desativado caso o recurso **Gerenciar as configurações e regras do Firewall do Windows** esteja desativado.

    Por padrão, o recurso é ativado e **Ativado** é selecionado.

  - Gerenciar as configurações e regras do Firewall do Windows.

Esse recurso ativa ou desativa o gerenciamento das configurações e regras do Firewall do Windows.

Caso a função esteja ativada, o aplicativo executa as seguintes ações:

- Faz a sondagem do Firewall do Windows em um intervalo de um minuto.
- Lê e copia as configurações do Firewall do Windows, inclusive as regras do firewall.
- Define os valores das configurações do Firewall do Windows para corresponder com as configurações da tarefa de Gerenciamento do Firewall.
- Cria uma lista de regras do firewall do Kaspersky Security Group no snap-in do Firewall do Windows. Esse conjunto contém todas as regras do firewall da tarefa de Gerenciamento de Firewall.

  Posteriormente, ao fazer a sondagem do Firewall do Windows, o aplicativo não sincroniza a lista de regras do firewall do Kaspersky Security Group com a lista de regras da tarefa Gerenciamento de Firewall. Para sincronizar as listas de regras do firewall é necessário reiniciar a tarefa de Gerenciamento de Firewall.
- Restringe a capacidade de editar as configurações e regras do Firewall do Windows com o uso de ferramentas de terceiros ou diretamente no snap-in (wf.msc). Caso as configurações ou regras do Firewall do Windows sejam alteradas, o aplicativo reverterá as alterações dentro de um minuto para os valores de configurações definidos usando a tarefa de Gerenciamento do Firewall.

Caso a função esteja desativada, o aplicativo restaura as configurações e regras do Firewall do Windows para os valores que o aplicativo salvou após a primeira sondagem do Firewall do Windows e não gerencia mais as configurações e regras do Firewall do Windows.

Esse recurso não pode ser desativado caso o recurso **Manter o estado do Firewall do Windows** esteja desativado.

Essa opção é ativada por padrão.

Sobre as Regras de Firewall

Caso o modo de interação com o Firewall do Windows esteja definido como **Controlar a operação do Firewall do Windows**, a tarefa Gerenciamento de Firewall filtra o tráfego de rede através do Firewall do Windows usando as regras do firewall.

As regras do firewall para aplicativos controlam as conexões de rede para aplicativos especificados. O critério para acionamento dessas regras baseia-se em um caminho para um arquivo executável do aplicativo.

As regras de porta do firewall controlam as conexões de rede para portas e protocolos especificados (TCP/UDP). Os critérios de acionamento dessas regras são a porta ou o intervalo de portas e o tipo de protocolo.

As regras de porta envolvem um escopo mais amplo do que as de aplicativo. Ao permitir as conexões de acordo com as regras de porta, o nível de segurança do dispositivo protegido é reduzido.

É possível gerenciar as regras do firewall:

- criar e excluir regras do firewall

- alterar as configurações das regras do firewall
- ativar ou desativar as regras do firewall

Regras do firewall criadas por padrão

Durante a instalação, o Kaspersky Embedded Systems Security for Windows cria um conjunto de regras de permissão para impedir o bloqueio de aplicativos instalados juntamente com o Kaspersky Embedded Systems Security for Windows. Veja abaixo os detalhes e as limitações.

Quando instalado em um dispositivo com qualquer versão compatível do Windows, o Kaspersky Embedded Systems Security for Windows cria um conjunto de regras para conexões de rede de entrada:

- Regras de permissão para o Console do Kaspersky Embedded Systems Security for Windows, localizado na pasta de instalação do aplicativo. Estado: ativado. Escopo da regra: todos os endereços. Protocolos: TCP e UPD (uma regra por protocolo).
- Duas regras de permissão para a porta local 15000, caso o Agente de Rede do Kaspersky Security Center esteja instalado no dispositivo. Estado: ativado. Escopo da regra: todos os endereços. Protocolos: TCP e UPD (uma regra por protocolo).

Ao ser instalado em um dispositivo com Windows 7 ou superior, o Kaspersky Embedded Systems Security for Windows cria um conjunto de regras para as conexões de rede de saída:

- Regras de permissão para o Console do Kaspersky Embedded Systems Security for Windows (kavfsgt.exe), localizado na pasta de instalação do aplicativo. Estado: ativado. Escopo da regra: todos os endereços. Protocolos: TCP e UPD (uma regra por protocolo).
- Regras de permissão para o Kaspersky Embedded Systems Security for Windows, (kavfswp.exe), localizado na pasta de instalação do aplicativo. Estado: ativado. Escopo da regra: todos os endereços. Protocolos: TCP e UPD (uma regra por protocolo).
- Duas regras de permissão para a porta local 13000, caso o Agente de Rede do Kaspersky Security Center esteja instalado no dispositivo. Estado: ativado. Escopo da regra: todos os endereços. Protocolos: TCP e UPD (uma regra por protocolo).

Ao desinstalar o Kaspersky Embedded Systems Security for Windows, o aplicativo remove todas as regras de firewall criadas, exceto as regras criadas pelo Agente de Rede do Kaspersky Security Center, como o Kaspersky Security Center WDS e o Kaspersky Administration Kit. O aplicativo também remove as regras de ICMPv4 e ICMPv6 para Windows 7 e posterior.

Ao desinstalar o Kaspersky Embedded Systems Security for Windows, o aplicativo ativa todas as conexões ICMP para os sistemas operacionais anteriores ao Windows 7.

Configurações padrão da tarefa de Gerenciamento de Firewall

A tarefa de Gerenciamento de Firewall usa as configurações padrão descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Configurações padrão da tarefa de Gerenciamento de Firewall

Configuração	Valor padrão	Descrição
Modo de interação entre o Kaspersky Embedded Systems	**Observar o estado do**	O aplicativo monitora apenas o status do Firewall do Windows e envia uma notificação ao Kaspersky Security Center caso o Firewall do Windows esteja desativado.

Security for Windows e o Firewall do Windows	**Firewall do Windows**	
Conexões de entrada	**Bloquear**	É possível criar e configurar regras do firewall de entrada para bloquear ou permitir as conexões de entrada.
Conexões de saída	**Permitir**	É possível criar e configurar regras do firewall de conexões de saída para bloquear ou permitir as conexões de saída.
Permitir conexões ICMP	**Desativado**	Essa configuração permite conexões de rede de entrada e saída via ICMPv4 e ICMPv6, independentemente das configurações da tarefa para as conexões de entrada e saída.
Programação de inicialização da tarefa	N/A	A tarefa de Gerenciamento de Firewall não inicia automaticamente no momento da inicialização do Kaspersky Embedded Systems Security for Windows. Você pode configurar a programação de inicialização da tarefa.

Configuração da tarefa de Gerenciamento de Firewall usando o Plug-in de Administração

Esta seção fornece instruções sobre como definir as configurações gerais da tarefa Gerenciamento de Firewall, além de criar e configurar as regras do firewall com o uso do Plug-in de Administração.

Definição das configurações gerais da tarefa de Gerenciamento de Firewall

Para definir as configurações gerais da tarefa de Gerenciamento de Firewall com o uso do Plug-in de Administração:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Controle de atividades de rede**, na seção **Gerenciamento de firewall**, clique no botão **Configurações**.

   A janela **Gerenciamento de firewall** é exibida.
5. Na guia **Geral**, no bloco **Integração do Firewall do Windows**, selecione o modo de interação entre o Kaspersky Embedded Systems Security for Windows e o Firewall do Windows:

- **Observar o estado do Firewall do Windows**. Caso essa opção seja selecionada, o aplicativo monitorará apenas o status do Firewall do Windows e enviará um evento de aviso ao Kaspersky Security Center se o Firewall do Windows não estiver iniciado.

  Caso essa opção seja selecionada para substituir a opção **Controlar a operação do Firewall do Windows**, o aplicativo restaurará as configurações internas do Firewall do Windows na próxima vez que o sistema operacional do dispositivo protegido for iniciado.

- **Controlar a operação do Firewall do Windows**. Caso essa opção seja selecionada, o aplicativo monitorará o Firewall do Windows no nível determinado pelas seguintes configurações:

  - Manter o estado do Firewall do Windows.
  - Gerenciar as configurações e regras do Firewall do Windows.
  - Permitir conexões ICMP.

6. No bloco **Conexões de entrada**, defina as configurações para as conexões de rede de entrada:

   - Use a lista suspensa **Ação para conexões de entrada** para especificar a ação que o Firewall do Windows deverá executar para todas as conexões de rede de entrada, a menos que isso seja definido de outra forma nas regras do firewall para as conexões de entrada.

   - Caso necessário, adicione as regras do firewall para as conexões de entrada.

     As regras do firewall para as conexões de entrada executam a função de exclusões. Por exemplo, caso uma regra de permissão seja configurada para as conexões de rede de entrada e o usuário selecione **Bloquear** na lista suspensa **Ação para conexões de entrada**, o Firewall do Windows permitirá as conexões de rede de entrada que correspondam aos critérios da regra.

7. No bloco **Conexões de saída**, defina as configurações para as conexões de rede de saída:

   - Use a lista suspensa **Ação para conexões de saída** para especificar a ação que o Firewall do Windows deverá executar para todas as conexões de rede de saída, a menos que isso seja definido de outra forma nas regras do firewall para as conexões de saída.

   - Caso necessário, adicione as regras do firewall para as conexões de saída.

     As regras do firewall para as conexões de saída executam a função de exclusões. Por exemplo, caso uma regra de bloqueio seja configurada para as conexões de rede de saída e o usuário selecione **Permitir** na lista suspensa **Ação para conexões de saída**, o Firewall do Windows bloqueará as conexões de rede de saída que correspondam aos critérios da regra.

8. Clique no botão **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. A data e hora nas quais as configurações foram alteradas são salvas no log de auditoria do sistema.

Criando e configurando regras de Firewall

Para criar e configurar as regras do firewall usando o Plugin de Administração:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Controle de atividades de rede**, em **Gerenciamento de firewall**, clique no botão **Configurações**.

   A janela **Gerenciamento de firewall** é exibida.

5. Na guia **Geral**, na seção **Conexões de entrada**, clique no botão **Lista de regras**.

   A janela **Regras de firewall para conexões de entrada** é exibida.

6. Crie e configure as regras do firewall para as conexões de entrada.

1. Clique no botão **Adicionar** na guia **Aplicativos**.

   A janela **Regras de firewall para aplicativo** é exibida.

2. Defina as configurações da regra:

   a. No campo **Nome da regra**, digite o nome da regra.

   > O nome da regra não diferencia caracteres maiúsculos de minúsculos e não deve corresponder aos nomes reservados All, ICMPv4 e ICMPv6. Também deve ser exclusivo na lista de todas as regras para as conexões de rede de entrada.

   b. Na lista **Ação da regra**, selecione uma das seguintes opções:

   - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de entrada para o aplicativo.
   - **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de entrada para o aplicativo.

   c. No campo **Caminho do aplicativo**, especifique o caminho manualmente ou usando o botão **Procurar** para o arquivo executável do aplicativo para o qual a regra está sendo configurada.

   d. No campo **Ação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de entrada dos endereços de rede especificados, de acordo com as configurações da regra.

   > Você pode usar apenas endereços IPv4.

   e. Clique no botão **OK** para salvar a regra.

3. Clique no botão **Adicionar** na guia **Portas**.

   A janela **Regras de firewall para portas** é exibida.

4. Defina as configurações da regra:

   a. No campo **Nome da regra**, digite o nome da regra.

   b. Na lista **Ação da regra**, selecione uma das seguintes opções:

   - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de entrada para as portas.
   - **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de entrada para as portas.

   c. No bloco **Portas locais**, especifique uma porta ou um intervalo de portas.

   d. Selecione o tipo de protocolo (TCP/UDP) para o qual o aplicativo permitirá as conexões.

   e. No campo **Ação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de entrada dos endereços de rede especificados, de acordo com as configurações da regra.

Você pode usar apenas endereços IPv4.

f. Clique no botão **OK** para salvar a regra.

5. Na janela **Regras de firewall para conexões de entrada**, clique no botão **OK**.

7. Na guia **Geral**, no bloco **Conexões de saída**, clique no botão **Lista de regras**.
   A janela **Regras de firewall para conexões de saída** é exibida.

8. Crie e configure as regras do firewall para as conexões de saída.

1. Clique no botão **Adicionar** na guia **Aplicativos**.

   A janela **Regras de firewall para aplicativo** é exibida.

2. Defina as configurações da regra:

   a. No campo **Nome da regra**, digite o nome da regra.

   > O nome da regra, independentemente de os caracteres serem maiúsculos ou minúsculos, não deve corresponder aos nomes reservados All, ICMPv4 e ICMPv6; ela deve ser exclusiva na lista de todas as regras para as conexões de rede de saída.

   b. Na lista **Ação da regra**, selecione uma das seguintes opções:

   - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de saída para o aplicativo.
   - **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de saída para o aplicativo.

   c. No campo **Caminho do aplicativo**, especifique o caminho manualmente ou usando o botão **Procurar** para o arquivo executável do aplicativo para o qual a regra está sendo configurada.

   d. No campo **Ação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de saída para os endereços de rede especificados de acordo com as configurações da regra.

   > Você pode usar apenas endereços IPv4.

   e. Clique no botão **OK** para salvar a regra.

3. Clique no botão **Adicionar** na guia **Portas**.

   A janela **Regras de firewall para portas** é exibida.

4. Defina as configurações da regra:

   a. No campo **Nome da regra**, digite o nome da regra.

   b. Na lista **Ação da regra**, selecione uma das seguintes opções:

   - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de saída para as portas.
   - **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de saída para as portas.

   c. No bloco **Portas remotas**, especifique uma porta ou um intervalo de portas.

   d. Selecione o tipo de protocolo (TCP/UDP) para o qual o aplicativo controlará as conexões de saída.

   e. No campo **Ação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de saída para os endereços de rede especificados de acordo com as configurações da regra.

Você pode usar apenas endereços IPv4.

f. Clique no botão **OK** para salvar a regra.

5. Na janela **Regras de firewall para conexões de saída**, clique no botão **OK**.

9. Clique no botão **OK** na janela **Gerenciamento de firewall**.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. A data e hora nas quais as configurações foram alteradas são salvas no log de auditoria do sistema.

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 node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Controle de atividades de rede**, clique no botão **Configurações** na subseção **Gerenciamento de firewall**.
5. Clique no botão **Lista de regras** na janela que se abre.

   A janela **Regras de firewall para conexões de entrada** é exibida.
6. Dependendo do tipo da regra cujo status deseja modificar, clique no link de **Entrada** ou **Saída**, depois selecione os **Aplicativos** ou a guia **Portas**.
7. 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.
8. Clique no botão **OK** na janela **Regras de firewall para conexões de entrada**.
9. Clique no botão **OK** na janela **Gerenciamento de firewall**.
10. Clique no botão **OK** na janela **Propriedades: <Nome da política>**.

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 node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Controle de atividades de rede**, clique no botão **Configurações** na subseção **Gerenciamento de firewall**.
5. Clique no botão **Lista de regras** na janela que se abre.

   A janela **Regras de firewall para conexões de entrada** é exibida.
6. Dependendo do tipo da regra cujo status deseja modificar, selecione a guia **Aplicativos** ou **Portas**.
7. Na lista de regras, selecione a regra que você deseja excluir.
8. Clique no botão **Excluir**.

   A regra selecionada é excluída.
9. Clique no botão **OK** na janela **Regras de firewall para conexões de entrada**.
10. Clique no botão **OK** na janela **Gerenciamento de firewall**.
11. Clique no botão **OK** na janela **Propriedades: <Nome da política>**.

As configurações da tarefa de Gerenciamento de Firewall especificadas são salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Configuração da tarefa de Gerenciamento de Firewall usando o Console do Aplicativo

Esta seção fornece instruções sobre como definir as configurações gerais da tarefa Gerenciamento de Firewall, além de criar e configurar as regras do firewall com o uso da interface do Console do Aplicativo.

Definição das configurações gerais da tarefa de Gerenciamento de Firewall

Algumas configurações de regras do firewall para as conexões de entrada e saída podem estar indisponíveis se o Console do Aplicativo estiver conectado ao host local (no qual ele foi iniciado) e as configurações não forem compatíveis com o sistema operacional do host.

Para definir as configurações gerais da tarefa Gerenciamento de firewall com o uso do Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o nó **Controle do Computador**.
2. Selecionar o node secundário **Gerenciamento de firewall**.
3. Clique no link **Parâmetros** no painel de detalhes do nó **Gerenciamento de firewall**.

   A janela **Configurações da tarefa** é aberta.
4. Na guia **Geral**, no bloco **Filtragem do tráfego de rede**, selecione a opção de interação entre o Kaspersky Embedded Systems Security for Windows e o Firewall do Windows:

   - **Observar o estado do Firewall do Windows**. Caso essa opção seja selecionada, o aplicativo monitorará apenas o status do Firewall do Windows e enviará um evento de aviso ao Kaspersky Security Center se o Firewall do Windows não estiver iniciado.

     Caso essa opção seja selecionada para substituir a opção **Controlar a operação do Firewall do Windows**, o aplicativo restaurará as configurações internas do Firewall do Windows na próxima vez que o sistema operacional do dispositivo protegido for iniciado.

   - **Controlar a operação do Firewall do Windows**. Caso essa opção seja selecionada, o aplicativo monitorará o Firewall do Windows no nível determinado pelas seguintes configurações:

     - Manter o estado do Firewall do Windows.
     - Gerenciar as configurações e regras do Firewall do Windows.
     - Permitir conexões ICMP.
5. No bloco **O programa controla a operação do Firewall do Windows de acordo com as configurações abaixo**, defina as seguintes configurações:

   - Use a lista suspensa **Ação para conexões de entrada** para especificar a ação que o Firewall do Windows deverá executar para todas as conexões de rede de entrada, a menos que isso seja definido de outra forma nas regras do firewall para as conexões de entrada.
   - Caso necessário, adicione as regras do firewall para as conexões de entrada.

     As regras do firewall para as conexões de entrada executam a função de exclusões. Por exemplo, caso uma regra de permissão seja configurada para as conexões de rede de entrada e o usuário selecione **Bloquear** na lista suspensa **Ação para conexões de entrada**, o Firewall do Windows permitirá as conexões de rede de entrada que correspondam aos critérios da regra.
   - Use a lista suspensa **Ação para conexões de saída** para especificar a ação que o Firewall do Windows deverá executar para todas as conexões de rede de saída, a menos que isso seja definido de outra forma nas regras do firewall para as conexões de saída.
   - Caso necessário, adicione as regras do firewall para as conexões de saída.

As regras do firewall para as conexões de saída executam a função de exclusões. Por exemplo, caso uma regra de bloqueio seja configurada para as conexões de rede de saída e o usuário selecione **Permitir** na lista suspensa **Ação para conexões de saída**, o Firewall do Windows bloqueará as conexões de rede de saída que correspondam aos critérios da regra.

6. Clique no botão **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. A data e hora nas quais as configurações foram alteradas são salvas no log de auditoria do sistema.

Criação e configuração das regras de Firewall

Para criar e configurar as regras do firewall com o uso do Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o nó **Controle do Computador**.
2. Selecionar o node secundário **Gerenciamento de firewall**.
3. Clique no link **Entrada** no painel de detalhes do nó **Gerenciamento de firewall**.

   A janela **Regras de firewall para conexões de entrada** é exibida.
4. Crie e configure as regras do firewall para as conexões de entrada.

1. Clique no botão **Adicionar** na guia **Aplicativos**.

   A janela **Regras de firewall para aplicativo** é exibida.

2. Defina as configurações da regra:

   a. No campo **Nome da regra**, digite o nome da regra.

   > O nome da regra, independentemente de os caracteres serem maiúsculos ou minúsculos, não deve corresponder aos nomes reservados Todos, ICMPv4 e ICMPv6; ela deve ser exclusiva na lista de todas as regras para as conexões de rede de entrada.

   b. Na lista **Ação da regra**, selecione uma das seguintes opções:

   - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de entrada para o aplicativo.
   - **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de entrada para o aplicativo.

   c. No campo **Caminho do aplicativo**, especifique o caminho manualmente ou usando o botão **Procurar** para o arquivo executável do aplicativo para o qual a regra está sendo configurada.

   d. No campo **Ação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de entrada dos endereços de rede especificados de acordo com as configurações da regra.

   > Você pode usar apenas endereços IPv4.

   e. Clique no botão **OK** para salvar a regra.

3. Clique no botão **Adicionar** na guia **Portas**.

   A janela **Regras de firewall para portas** é exibida.

4. Defina as configurações da regra:

   a. No campo **Nome da regra**, digite o nome da regra.

   b. Na lista **Ação da regra**, selecione uma das seguintes opções:

   - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de entrada para as portas.
   - **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de entrada para as portas.

   c. No bloco **Portas locais**, especifique uma porta ou um intervalo de portas.

   d. Selecione o tipo de protocolo (TCP/UDP) para o qual o aplicativo permitirá as conexões.

   e. No campo **Ação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de entrada dos endereços de rede especificados de acordo com as configurações da regra.

Você pode usar apenas endereços IPv4.

f. Clique no botão **OK** para salvar a regra.

5. Na janela **Regras de firewall para conexões de entrada**, clique no botão **OK**.

5. Clique no link **Conexões de saída** no painel de detalhes do nó **Gerenciamento de firewall**.

   A janela **Regras de firewall para conexões de saída** é exibida.

6. Crie e configure as regras do firewall para as conexões de saída.

1. Clique no botão **Adicionar** na guia **Aplicativos**.

   A janela **Regras de firewall para aplicativo** é exibida.

2. Defina as configurações da regra:

   a. No campo **Nome da regra**, digite o nome da regra.

   > O nome da regra, independentemente de os caracteres serem maiúsculos ou minúsculos, não deve corresponder aos nomes reservados Todos, ICMPv4 e ICMPv6; ela deve ser exclusiva na lista de todas as regras para as conexões de rede de saída.

   b. Na lista **Ação da regra**, selecione uma das seguintes opções:

   - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de saída para o aplicativo.
   - **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de saída para o aplicativo.

   c. No campo **Caminho do aplicativo**, especifique o caminho manualmente ou usando o botão **Procurar** para o arquivo executável do aplicativo para o qual a regra está sendo configurada.

   d. No campo **Ação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de saída para os endereços de rede especificados de acordo com as configurações da regra.

   > Você pode usar apenas endereços IPv4.

   e. Clique no botão **OK** para salvar a regra.

3. Clique no botão **Adicionar** na guia **Portas**.

   A janela **Regras de firewall para portas** é exibida.

4. Defina as configurações da regra:

   a. No campo **Nome da regra**, digite o nome da regra.

   b. Na lista **Ação da regra**, selecione uma das seguintes opções:

   - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de saída para as portas.
   - **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de saída para as portas.

   c. No bloco **Portas remotas**, especifique uma porta ou um intervalo de portas.

   d. Selecione o tipo de protocolo (TCP/UDP) para o qual o aplicativo controlará as conexões de saída.

   e. No campo **Ação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de saída para os endereços de rede especificados de acordo com as configurações da regra.

Você pode usar apenas endereços IPv4.

f. Clique no botão **OK** para salvar a regra.

5. Na janela **Regras de firewall para conexões de saída**, clique no botão **OK**.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. A data e hora em que as configurações da tarefa foram alteradas são salvas no log de auditoria do sistema.

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. Na árvore do Console do Aplicativo, expanda o node **Controle do Computador**.
2. Selecionar o node secundário **Gerenciamento de firewall**.
3. Clique no link **Gerenciamento de firewall** no painel de detalhes do nó **Regras de firewall**.

   A janela **Regras de firewall** é exibida.
4. Dependendo do tipo da regra cujo status deseja modificar, clique no link de **Entrada** ou **Saída**, depois selecione os **Aplicativos** ou a guia **Portas**.
5. 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.
6. Clique no botão **Regras de firewall** na janela **Salvar**.

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. Na árvore do Console do Aplicativo, expanda o node **Controle do Computador**.
2. Selecionar o node secundário **Gerenciamento de firewall**.
3. Clique no link **Gerenciamento de firewall** no painel de detalhes do nó **Regras de firewall**.

A janela **Regras de firewall** é exibida.

4. Dependendo do tipo da regra cujo status deseja modificar, selecione a guia **Aplicativos** ou **Portas**.
5. Na lista de regras, selecione a regra que você deseja excluir.
6. Clique no botão **Excluir**.

   A regra selecionada é excluída.
7. Clique no botão **Regras de firewall** na janela **Salvar**.

As configurações da tarefa especificadas serão salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Configuração da tarefa de Gerenciamento de Firewall usando o Plug-in da Web

Esta seção fornece instruções sobre como definir as configurações gerais da tarefa Gerenciamento de Firewall, além de criar e configurar as regras do firewall com o uso do Plug-in da Web.

Definição das configurações gerais da tarefa de Gerenciamento de Firewall

Para definir as configurações gerais da tarefa Gerenciamento de Firewall com o uso do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Controle de atividades de rede**.
5. Clique no botão **Configurações** na seção **Gerenciamento de Firewall**.

   A janela **Gerenciamento de Firewall** é exibida.
6. Na guia **Geral**, no bloco **Integração do Firewall do Windows**, selecione a opção de interação entre o Kaspersky Embedded Systems Security for Windows e o Firewall do Windows:

   - **Observar o estado do Firewall do Windows O programa apenas observa o estado do Firewall do Windows**. Caso essa opção seja selecionada, o aplicativo monitorará apenas o status do Firewall do Windows e enviará um evento de aviso ao Kaspersky Security Center se o Firewall do Windows não estiver iniciado.

     Caso essa opção seja selecionada para substituir a opção **Controlar a operação do Firewall do Windows O programa controla a operação do Firewall do Windows de acordo com as configurações abaixo**, o aplicativo restaurará as configurações internas do Firewall do Windows na próxima vez que o sistema operacional do dispositivo protegido for iniciado.

   - **Controlar a operação do Firewall do Windows O programa controla a operação do Firewall do Windows de acordo com as configurações abaixo**. Caso essa opção seja selecionada, o aplicativo monitorará o Firewall do Windows no nível determinado pelas seguintes configurações:

- Manter o estado do Firewall do Windows.
- Gerenciar as configurações e regras do Firewall do Windows.
- Permitir conexões ICMP.

7. No bloco **Conexões de entrada**, defina as configurações para as conexões de rede de entrada:

   - Use a lista suspensa **Ação para conexões de entrada** para especificar a ação que o Firewall do Windows deverá executar para todas as conexões de rede de entrada, a menos que isso seja definido de outra forma nas regras do firewall para as conexões de entrada.
   - Caso necessário, adicione as regras do firewall para as conexões de entrada.

     As regras do firewall para as conexões de entrada executam a função de exclusões. Por exemplo, caso uma regra de permissão seja configurada para as conexões de rede de entrada e o usuário selecione **Bloquear** na lista suspensa **Ação para conexões de entrada**, o Firewall do Windows permitirá as conexões de rede de entrada que correspondam aos critérios da regra.

8. No bloco **Conexões de saída**, defina as configurações para as conexões de rede de saída:

   - Use a lista suspensa **Ação para conexões de saída** para especificar a ação que o Firewall do Windows deverá executar para todas as conexões de rede de saída, a menos que isso seja definido de outra forma nas regras do firewall para as conexões de saída.
   - Caso necessário, adicione as regras do firewall para as conexões de saída.

     As regras do firewall para as conexões de saída executam a função de exclusões. Por exemplo, caso uma regra de bloqueio seja configurada para as conexões de rede de saída e o usuário selecione **Permitir** na lista suspensa **Ação para conexões de saída**, o Firewall do Windows bloqueará as conexões de rede de saída que correspondam aos critérios da regra.

9. Clique no botão **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. A data e hora nas quais as configurações foram alteradas são salvas no log de auditoria do sistema.

Configuração	Descrição
Regras de firewall para aplicativos	É possível gerenciar as regras do aplicativo. Este tipo de regra permite conexões direcionadas de rede para aplicativos especificados. O critério para acionamento dessas regras baseia-se em um caminho para um arquivo executável.
Regras de firewall para portas	É possível gerenciar as regras de portas. Este tipo de regra permite conexões de rede para portas e protocolos (TCP/UDP) especificados. Os critérios para acionamento destas regras baseiam-se no número da porta e tipo de protocolo.
Gerenciamento da tarefa	É possível definir configurações para a inicialização programada da tarefa.

Criação e configuração das regras de Firewall

Para criar e configurar as regras do firewall com o uso do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Controle de atividades de rede**.
5. Clique no botão **Configurações** no bloco **Gerenciamento de Firewall**.
   A janela **Gerenciamento de Firewall** é exibida.
6. Crie e configure uma regra do firewall de entrada para o aplicativo.
   a. Selecione a guia **Aplicativos (conexões de entrada)**.
   b. Clique no botão **Adicionar**.
   c. Na parte direita da janela, marque a caixa de seleção **Usar a regra** para ativar a regra.
   d. No campo **Nome da regra**, digite o nome da regra.

      O nome da regra, independentemente de os caracteres serem maiúsculos ou minúsculos, não deve corresponder aos nomes reservados Todos, ICMPv4 e ICMPv6; ela deve ser exclusiva na lista de todas as regras para as conexões de rede de entrada para aplicativos.

   e. Na lista **Ação da regra**, selecione uma das seguintes opções:
      - **Permitir.** Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de entrada para o aplicativo.
      - **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de entrada para o aplicativo.

   f. No campo **Caminho do aplicativo**, especifique o caminho manualmente para o arquivo executável do aplicativo para o qual a regra está sendo configurada.
   g. No campo **Escopo de aplicação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de entrada dos endereços de rede especificados de acordo com as configurações da regra.

      Você pode usar apenas endereços IPv4.

   h. Clique no botão **OK** para salvar a regra.
7. Crie e configure uma regra do firewall para as conexões de entrada para portas.

a. Selecione a guia **Portas (conexões de entrada)**.

b. Clique no botão **Adicionar**.

c. Na parte direita da janela, marque a caixa de seleção **Usar a regra** para ativar a regra.

d. No campo **Nome da regra**, digite o nome da regra.

> O nome da regra, independentemente de os caracteres serem maiúsculos ou minúsculos, não deve corresponder aos nomes reservados Todos, ICMPv4 e ICMPv6; ela deve ser exclusiva na lista de todas as regras para as conexões de rede de entrada para portas.

e. Na lista **Ação da regra**, selecione uma das seguintes opções:

- **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de entrada para as portas.
- **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de entrada para as portas.

f. No bloco **Portas locais**, especifique uma porta ou um intervalo de portas.

g. Selecione o tipo de protocolo (TCP/UDP) para o qual o aplicativo permitirá as conexões.

h. No campo **Escopo de aplicação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de entrada dos endereços de rede especificados de acordo com as configurações da regra.

> Você pode usar apenas endereços IPv4.

i. Clique no botão **OK** para salvar a regra.

8. Crie e configure uma regra do firewall de saída para o aplicativo.

a. Selecione a guia **Aplicativos (conexões de saída)**.

b. Clique no botão **Adicionar**.

c. Na parte direita da janela, marque a caixa de seleção **Usar a regra** para ativar a regra.

d. No campo **Nome da regra**, digite o nome da regra.

> O nome da regra, independentemente de os caracteres serem maiúsculos ou minúsculos, não deve corresponder aos nomes reservados Todos, ICMPv4 e ICMPv6; ela deve ser exclusiva na lista de todas as regras para as conexões de rede de saída para aplicativos.

e. Na lista **Ação da regra**, selecione uma das seguintes opções:

- **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de saída para o aplicativo.
- **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de saída para o aplicativo.

f. No campo **Caminho do aplicativo**, especifique o caminho manualmente para o arquivo executável do aplicativo para o qual a regra está sendo configurada.

g. No campo **Escopo de aplicação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de saída dos endereços de rede especificados de acordo com as configurações da regra.

> Você pode usar apenas endereços IPv4.

h. Clique no botão **OK** para salvar a regra.

9. Crie e configure uma regra do firewall de saída para portas.

a. Selecione a guia **Portas (conexões de saída)**.

b. Clique no botão **Adicionar**.

c. Na parte direita da janela, marque a caixa de seleção **Usar a regra** para ativar a regra.

d. No campo **Nome da regra**, digite o nome da regra.

O nome da regra, independentemente de os caracteres serem maiúsculos ou minúsculos, não deve corresponder aos nomes reservados Todos, ICMPv4 e ICMPv6; ela deve ser exclusiva na lista de todas as regras para as conexões de rede de saída para portas.

e. Na lista **Ação da regra**, selecione uma das seguintes opções:

- **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de saída para as portas.
- **Bloquear**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de saída para as portas.

f. No bloco **Portas remotas**, especifique uma porta ou um intervalo de portas.

g. Selecione o tipo de protocolo (TCP/UDP) para o qual o aplicativo permitirá as conexões.

h. No campo **Escopo de aplicação da regra**, especifique os endereços de rede. O aplicativo monitora as conexões de saída para os endereços de rede especificados de acordo com as configurações da regra.

Você pode usar apenas endereços IPv4.

i. Clique no botão **OK** para salvar a regra.

10. Clique no botão **OK** na janela **Gerenciamento de Firewall**.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. A data e hora nas quais as configurações foram alteradas são salvas no log de auditoria do sistema.

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. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Controle de atividades de rede**.

5. Clique no botão **Configurações** na subseção **Gerenciamento de Firewall**.

6. Dependendo do tipo da regra cujo status deseja modificar, selecione a guia **Regras de firewall para aplicativos** ou **Regras de firewall para portas**.

7. 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, ative o botão à esquerda do nome da regra.
   - Se você quiser desativar uma regra ativada, desative o botão à esquerda do nome da regra.

8. Clique no botão **OK**.

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. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos → Políticas e perfis**.

2. Clique no nome da política que você quer configurar.

3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.

4. Selecione a seção **Controle de atividades de rede**.

5. Clique no botão **Configurações** na subseção **Gerenciamento de Firewall**.

6. Dependendo do tipo da regra que você deseja excluir, selecione a guia **Regras de firewall para aplicativos** ou **Regras de firewall para portas**.

7. Na lista de regras, selecione a regra que você deseja excluir.

8. Clique no botão **Excluir**.

   A regra selecionada é excluída.

9. Clique no botão **OK**.

As configurações da tarefa especificadas serão salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Monitor de Integridade de Arquivos

Esta seção contém informações sobre a inicialização e a configuração da tarefa Monitor de Integridade de Arquivos.

Sobre a tarefa Monitor de Integridade de Arquivos

A tarefa de 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 dispositivo 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 de monitoramento fica temporariamente fora do escopo da tarefa, por exemplo, se a tarefa for interrompida ou um dispositivo externo não estiver fisicamente presente em um dispositivo protegido. O Kaspersky Embedded Systems Security for Windows informa sobre operações de arquivos detectadas no escopo de monitoramento assim que um dispositivo externo 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 será executada.

Requisitos no ambiente

Para iniciar a tarefa de Monitor de Integridade de Arquivos, as seguintes condições devem ser atendidas:

- Os sistemas de arquivos ReFS ou NTFS devem ser utilizados no dispositivo 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 a criação de uma regra 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

É possível criar escopos de monitoramento excluídos. 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 as regras de monitoramento de operações de arquivos

A tarefa do Monitor de Integridade do Sistema é executada de acordo com as 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 de eventos de operações de arquivo detectados e registrados 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 do 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 do evento ao criar uma lista de usuários confiáveis nas configurações da regra de monitoramento de operações de arquivos.

Usuário não confiável é um status atribuído a qualquer usuário não indicado na lista de usuário confiável nas configurações da regra de escopo de monitoramento. Se o Kaspersky Embedded Systems Security for Windows detectar uma operação de arquivo realizada por um usuário não confiável, a tarefa de Monitor de Integridade de Arquivos registrará um Evento crítico no Log de tarefas.

Usuário confiável é um status atribuído para um usuário ou grupo de usuários autorizados a realizar operações de arquivo no escopo de monitoramento especificado. Se o Kaspersky Embedded Systems Security for Windows detectar operações de arquivo realizadas por um usuário confiável, a tarefa de Monitor de Integridade de Arquivos registrará um Evento informativo no Log de tarefas.

O Kaspersky Embedded Systems Security for Windows não é capaz de determinar os usuários que iniciam operações durante interrupções no monitoramento. Neste caso, o status do usuário é determinado como desconhecido.

Usuário desconhecido é um status atribuído a um usuário se o Kaspersky Embedded Systems Security for Windows 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 for Windows detectar uma operação de arquivo realizada por um usuário desconhecido, a tarefa de Monitor de Integridade de Arquivos registrará um evento de *Aviso* no Log de tarefas.

Marcadores de operação do arquivo

Quando a tarefa de Monitor de Integridade de Arquivos for executada, o Kaspersky Embedded Systems Security for Windows usará os marcadores de operação do arquivo para determinar se uma ação foi realizada em um arquivo.

Um marcador de operações de arquivos é um descritor único 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 operações de arquivos. 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 do arquivo selecionados ou do número de eventos.

Por padrão, o Kaspersky Embedded Systems Security for Windows considera todos os marcadores de operações de arquivos disponíveis. É possível selecionar marcadores de operação do arquivo manualmente nas configurações de regra da tarefa.

Considerar marcadores de operação do arquivo

ID de operação de arquivo	Marcador de operações de arquivos	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
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	NTFS, ReFS

	alterado	
TRANSACTED_CHANGE	Fluxo de arquivo nomeado alterado pela transação TxF	Somente ReFS

Configurações padrão da tarefa Monitor de Integridade de Arquivos

Por padrão, a tarefa de Monitor de Integridade de Arquivos tem as configurações descritas na tabela abaixo. É possível alterar os valores das configurações nos seguintes componentes:

- O Plug-in de Administração
- O Console do Aplicativo
- O Plug-in da Web

Configurações padrão da tarefa Monitor de Integridade de Arquivos

Configuração	Valor padrão	Descrição
Escopo de monitoramento	Não definido	Use essa opção para 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.
Usuários confiáveis confiáveis	Não definido	Use essa opção para especificar usuários e/ou grupos de usuários cujas ações nas pastas especificadas serão tratadas como seguras pelo componente.
Registrar informações sobre operações de arquivo que aparecem durante o período de interrupção do monitoramento	Usada	Essa configuração é usada para ativar ou desativar o registro de operações de arquivo executadas nos escopos de monitoramento especificados durante os períodos em que a tarefa está ociosa. Por padrão, as estatísticas são coletadas para usuários e objetos não confiáveis e desconhecidos.
Bloquear tentativas de comprometer o log USN	Usada	Use essa opção para ativar ou desativar proteção do log USN.
Detectar e bloquear todas as operações de arquivos na área selecionada	Desativado	Marque ou desmarque a caixa de seleção **Detectar e bloquear todas as operações de arquivos na área selecionada** para bloquear todas as alterações para o escopo de monitoramento selecionado.
Excluir as seguintes pastas do controle	Não aplicado	Use essa opção para verificar o uso de exclusões das pastas onde as operações de arquivo não precisam ser monitoradas. Quando a tarefa de Monitor de Integridade de Arquivos for executada, o Kaspersky Embedded Systems Security for Windows ignorará os escopos de monitoramento especificados como exclusões.
Cálculo da soma de verificação	Não aplicado	Use essa opção para configurar o cálculo da soma de verificação do arquivo depois que as alterações forem feitas nele.
Definir marcadores de operações do	Todos os marcadores	Use esta opção para especificar o conjunto de marcadores de operação de arquivo. Se uma operação de arquivo executada

arquivo	de operação do arquivo disponíveis serão considerados	em um escopo de monitoramento for caracterizada por um ou mais marcadores especificados, ao Kaspersky Embedded Systems Security for Windows gerará um evento de auditoria.
Programação de inicialização da tarefa	A primeira execução não está programada.	É possível definir configurações para a inicialização programada da tarefa.

Gerenciamento do Monitor de Integridade de Arquivos por meio do Plug-in de Administração

Nesta seção, saiba como configurar a tarefa de Monitor de Integridade de Arquivos por meio do Plug-in de Administração.

Configuração da tarefa de Monitor de Integridade de Arquivos

Para definir as configurações da tarefa Monitor de Integridade do Sistema usando o Plug-in de Administração:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Inspeção do sistema**, no bloco **Monitor de Integridade de Arquivos**, clique no botão **Configurações**.

   A janela **Monitor de Integridade de Arquivos** é exibida.
5. Na guia **Definição de operação de monitoramento de arquivo**, defina as seguintes configurações:
   - Desmarque ou marque a caixa de seleção **Registrar informações sobre operações de arquivo que aparecem durante o período de interrupção do monitoramento**.

A caixa de seleção ativa ou desativa o monitoramento das operações do arquivo especificadas nas configurações da tarefa de Monitor de Integridade de Arquivos quando a tarefa não está em execução por alguma razão (remoção de um disco rígido, tarefa interrompida pelo usuário, erro de software).

Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows registrará eventos em todos os escopos de monitoramento quando a tarefa Monitor de Integridade de Arquivos não estiver em execução.

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 marcada por padrão.

- Desmarque ou marque a caixa de seleção **Bloquear tentativas de comprometer o log USN**.

  A caixa de seleção ativa ou desativa a proteção do log de USN.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security for Windows bloqueará as tentativas de excluir o log de USN ou comprometer seu conteúdo.

  Se a caixa de seleção estiver desmarcada, o aplicativo não monitorará as alterações do log de USN.

  A caixa de seleção é marcada por padrão.

6. Adicione as regras de monitoramento de operações de arquivos que determinarão o que a tarefa fará.
7. Na guia **Gerenciamento da tarefa**, defina as configurações para o início da tarefa programada.
8. Clique no botão **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. As informações sobre a data e hora da modificação das configurações são salvas no log de auditoria do sistema.

Criação e configuração de uma regra de monitoramento de operações de arquivos

Para criar e configurar uma regra de monitoramento de operações de arquivos com o uso do Plug-in de Administração:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Execute uma das seguintes ações:

   - Caso esteja criando uma regra de monitoramento de operações de arquivos em uma política, na seção **Inspeção do sistema** no bloco **Monitor de Integridade de Arquivos**, clique no botão **Configurações**.

A janela **Monitor de Integridade de Arquivos** é aberta na guia **Definição de operação de monitoramento de arquivo**.

- Caso esteja criando uma regra de monitoramento de operações de arquivos para uma tarefa local, na janela **Propriedades: Monitor de Integridade do Sistema**, vá para a seção **Configurações**.

5. No bloco **Escopo de monitoramento**, clique no botão **Adicionar**.

   A janela **Regra de monitoramento de operações de arquivos** é exibida.

6. Adicione um escopo de monitoramento de uma das seguintes maneiras:

   - Caso queira selecionar uma pasta ou unidade pela da caixa de diálogo padrão do Microsoft Windows:

     a. Clique no botão **Procurar**.

        A janela padrão **Procurar pasta** do Microsoft Windows e exibida.

     b. Selecione a pasta cujas operações de arquivos deseja monitorar.

     c. 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 na pasta <\dir>
     - <\dir*\nome.ext> — todos os arquivos com o nome <nome> e a extensão <ext> na pasta <\dir> e todas as subpastas

   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 for Windows não adicionará o escopo de monitoramento especificado.

7. Caso necessário, especifique os usuários confiáveis:

   a. Na guia **Usuários confiáveis**, no menu de contexto do botão **Adicionar**, selecione o método para adicionar usuários confiáveis.

      A janela **Seleção de usuário ou grupo de usuários** é aberta.

   b. Selecione os usuários ou grupos de usuários para os quais as operações de arquivos são permitidas no escopo de monitoramento selecionado.

   c. Clique no botão **OK**.

   Por padrão, o Kaspersky Embedded Systems Security for Windows trata todos os usuários que não estejam na lista de usuários confiáveis como não confiáveis e gera eventos críticos para eles. Para usuários confiáveis, as estatísticas são compiladas.

8. Na guia **Marcadores de operação do arquivo**, caso necessário, especifique os marcadores de operações de arquivos que deseja monitorar:

   a. Selecione a opção **Detectar operações de arquivo com base nos seguintes marcadores**.

   b. Na lista de operações de arquivos disponíveis, selecione as caixas ao lado das operações que deseja monitorar.

   Por padrão, o Kaspersky Embedded Systems Security for Windows detecta todos os marcadores de operações de arquivos. A opção **Detectar operações de arquivo com base em todos os marcadores reconhecíveis** está selecionada.

9. Caso queira bloquear todas as operações de arquivo para o escopo selecionado, marque a caixa de seleção **Detectar e bloquear todas as operações de arquivos na área selecionada**.

10. Se quiser que o aplicativo calcule a soma de verificação de um arquivo após ele ter sido modificado:

    a. Selecione **Calcular a soma da verificação para o arquivo, se possível. A soma de verificação estará disponível para visualização no relatório de tarefa** relatório de tarefa.

    b. Na lista suspensa **Tipo de cálculo de soma de verificação**, selecione uma das opções:

    - **Hash MD5**
    - **Hash SHA256**.

11. Caso necessário, adicione pastas ou unidades a serem excluídas do escopo de monitoramento de operações do arquivo selecionado:

    a. Na guia **Exclusões**, marque a caixa de seleção **Excluir as seguintes pastas do controle**.

    b. Clique no botão **Adicionar**.

    A janela **Exclusão a partir do escopo controlado** é exibida.

    c. Clique no botão **Procurar**.

    A janela padrão **Procurar pasta** do Microsoft Windows e exibida.

    d. Selecione uma pasta ou unidade.

    e. Clique no botão **OK**.

    A pasta ou unidade especificada será exibida na lista de exclusões na guia **Exclusões**.

    Também é possível adicionar escopos de monitoramento de operações excluídos manualmente usando as mesmas máscaras usadas para especificar os escopos de monitoramento de operações.

12. Clique no botão **Regra de monitoramento de operações de arquivos** na janela **OK**.

A regra de monitoramento de operações de arquivos configurada é exibida na janela **Monitor de Integridade do Sistema / Propriedades: Monitor de Integridade do Sistema** no bloco **Escopo de monitoramento**.

Exportação e importação de regras de monitoramento de operações de arquivos

É possível exportar as regras de monitoramento de operações de arquivos criadas manualmente nas propriedades da tarefa Monitor de Integridade do Sistema para um arquivo XML.

É possível importar as regras de monitoramento de operações de arquivos anteriormente exportadas para um arquivo XML nas propriedades da tarefa Monitor de Integridade do Sistema.

Para exportar ou importar as regras de monitoramento de operações de arquivos usando o Plug-in de Administração:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Execute uma das seguintes ações:
   - Se quiser importar ou exportar as regras de monitoramento de operações de arquivos em uma política, na seção **Inspeção do sistema**, no bloco **Monitor de Integridade de Arquivos**, clique no botão **Configurações**.

     A janela **Monitor de Integridade de Arquivos** é aberta na guia **Definição de operação de monitoramento de arquivo**.
   - Se quiser importar ou exportar as regras de monitoramento de operações de arquivo para uma tarefa local, na janela **Propriedades: Monitor de Integridade do Sistema**, vá para a seção **Configurações**.
5. Exportar ou importar regras de monitoramento de operações de arquivos:
   - **Como exportar as regras de monitoramento de operações de arquivos**.

     1. No bloco **Escopo de monitoramento**, clique no botão **Exportar**.

        A janela padrão do Microsoft Windows **Salvar como** é exibida.
     2. Especifique o caminho para salvar um arquivo XML com as configurações das regras de monitoramento de operações de arquivos.
     3. Insira o nome do arquivo no campo correspondente.
     4. Clique no botão **Salvar**.

        O aplicativo salvará um arquivo XML com as configurações das regras de monitoramento de operações de arquivos no caminho especificado.

- Como importar as regras para as regras de monitoramento de operações de arquivos.

  1. No bloco **Escopo de monitoramento**, clique no botão **Importar**.
  2. No menu de contexto do botão **Importar**, selecione um dos valores:
     - **Mesclar com as regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas não são duplicadas. Se pelo menos uma configuração de regra for exclusiva, a regra será adicionada.
     - **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
     - **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas.

     A janela **Abrir** padrão do Microsoft Windows é exibida.
  3. Especifique o caminho para o arquivo XML com as configurações das regras de monitoramento de operações de arquivos.
  4. Clique no botão **Abrir**.

     Na janela **Monitor de Integridade do Sistema** / **Propriedades: Monitor de Integridade do Sistema**, as regras importadas serão exibidas no bloco **Escopo de monitoramento**.

6. Clique no botão **Salvar** para salvar as alterações.

Gerenciamento do Monitor de Integridade de Arquivos por meio do Console do Aplicativo

Nesta seção, saiba como configurar a tarefa de Monitor de Integridade de Arquivos por meio do Console do Aplicativo.

Configuração da tarefa de Monitor de Integridade de Arquivos

Para definir as configurações gerais da tarefa Monitor de Integridade do Sistema com o uso do Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o node **Inspeção do sistema**.
2. Selecione o node secundário do **Monitor de Integridade de Arquivos**.
3. Clique no link **Propriedades** no painel de resultados do node do **Monitor de Integridade de Arquivos**.

   A janela **Configurações de tarefa** é aberta.
4. Na guia **Geral**, defina as seguintes configurações:

a. Desmarque ou marque a caixa de seleção **Registrar informações sobre operações de arquivo que aparecem durante o período de interrupção do monitoramento**.

A caixa de seleção ativa ou desativa o monitoramento das operações do arquivo especificadas nas configurações da tarefa de Monitor de Integridade de Arquivos quando a tarefa não está em execução por alguma razão (remoção de um disco rígido, tarefa interrompida pelo usuário, erro de software).

Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows registrará eventos em todos os escopos de monitoramento quando a tarefa Monitor de Integridade de Arquivos não estiver em execução.

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 marcada por padrão.

b. Desmarque ou marque a caixa de seleção **Bloquear tentativas de comprometer o log USN**.

A caixa de seleção ativa ou desativa a proteção do log de USN.

Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security for Windows bloqueará as tentativas de excluir o log de USN ou comprometer seu conteúdo.

Se a caixa de seleção estiver desmarcada, o aplicativo não monitorará as alterações do log de USN.

A caixa de seleção é marcada por padrão.

5. Nas guias **Agendamento** e **Avançado**, configure a programação de inicialização da tarefa.

6. Clique no botão **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. As informações sobre a data e hora da modificação das configurações são salvas no log de auditoria do sistema.

Criação e configuração de uma regra de monitoramento de operações de arquivos

Para criar e configurar uma regra de monitoramento de operações de arquivos usando o Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o node **Inspeção do sistema**.

2. Selecione o node secundário do **Monitor de Integridade de Arquivos**.

3. Clique no link **Monitor de Integridade de Arquivos** no painel de resultados do node do **Regras de monitoramento de operações de arquivos**.

   A janela **Regras de monitoramento de operações de arquivos** é exibida.

4. Especifique o caminho para o escopo de monitoramento de operações de arquivos de uma das seguintes maneiras:

   - Caso queira selecionar uma pasta ou unidade pela da caixa de diálogo padrão do Microsoft Windows:

     a. No lado abandonado da janela, clique no botão **Procurar**.

        A janela padrão **Procurar pasta** do Microsoft Windows e exibida.

     b. Selecione a pasta cujas operações de arquivos deseja monitorar.

c. 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 na pasta <\dir>
  - <\dir*\nome.ext> — todos os arquivos com o nome <nome> e a extensão <ext> na pasta <\dir> e todas as subpastas

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 for Windows não adicionará o escopo de monitoramento especificado.

5. Clique no botão **Adicionar**.

   O escopo de monitoramento será exibido na lista à esquerda da janela **Regras de monitoramento de operações de arquivos**.

6. Caso necessário, especifique os usuários confiáveis:

   a. Na guia **Usuários confiáveis**, clique no botão **Adicionar**.

      A janela **Selecionar usuários ou grupos** padrão do Microsoft Windows é exibida.

   b. Selecione usuários ou grupos de usuários que terão permissão para executar as operações nos arquivos no escopo de monitoramento selecionado.

   c. Clique no botão **OK**.

Por padrão, o Kaspersky Embedded Systems Security for Windows trata todos os usuários que não estejam na lista de usuários confiáveis como não confiáveis e gera eventos críticos para eles. Para usuários confiáveis, as estatísticas são compiladas.

7. Na guia **Definir marcadores de operações do arquivo**, caso necessário, especifique os marcadores de operações de arquivos que deseja monitorar:

   a. Selecione a opção **Detectar operações de arquivo com base nos seguintes marcadores**.

   b. Na lista de operações de arquivos disponíveis, selecione as caixas ao lado das operações que deseja monitorar.

Por padrão, o Kaspersky Embedded Systems Security for Windows detecta todos os marcadores de operações de arquivos. A opção **Detectar operações de arquivo com base em todos os marcadores reconhecíveis** está selecionada.

8. Caso queira bloquear todas as operações de arquivos para o escopo de monitoramento selecionado, marque a caixa de seleção **Detectar e bloquear todas as operações de arquivos na área selecionada**.

9. Se quiser que o aplicativo calcule a soma de verificação de um arquivo após ele ter sido modificado:

   a. No bloco **Cálculo da soma de verificação**, selecione **Calcule a soma de verificação para uma versão final de arquivo, depois que o arquivo for alterado, se possível. A soma de verificação estará disponível para visualização no log de tarefas**. **A soma de verificação estará disponível para visualização na caixa de seleção no log de tarefas**.

   b. Na lista suspensa **Calcule a soma de verificação usando o algoritmo**, selecione uma das opções:

      - **Hash MD5**
      - **Hash SHA256**.

10. Caso necessário, adicione pastas ou unidades para excluir as operações de arquivo do monitoramento:

    a. Na guia **Definir exclusões**, marque a caixa de seleção **Considere o escopo de monitoramento excluído**.

    b. Clique no botão **Procurar**.

       A janela padrão **Procurar pasta** do Microsoft Windows e exibida.

    c. Selecione uma pasta ou unidade.

    d. Clique no botão **OK**.

    e. Clique no botão **Adicionar**.

    A pasta ou unidade especificada será exibida na lista de exclusões.

    > Também é possível adicionar escopos de monitoramento de operações excluídos manualmente usando as mesmas máscaras usadas para especificar os escopos de monitoramento de operações.

11. Clique no botão **Salvar**.

Exportação e importação de regras de monitoramento de operações de arquivos

É possível exportar as regras de monitoramento de operações de arquivos criadas manualmente nas propriedades da tarefa Monitor de Integridade do Sistema para um arquivo XML.

É possível importar as regras de monitoramento de operações de arquivos anteriormente exportadas para um arquivo XML nas propriedades da tarefa Monitor de Integridade do Sistema.

Para exportar ou importar as regras de monitoramento de operações de arquivos usando o Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o node **Inspeção do sistema**.
2. Selecione o node secundário do **Monitor de Integridade de Arquivos**.
3. Clique no link **Monitor de Integridade de Arquivos** no painel de resultados do node do **Regras de monitoramento de operações de arquivos**.

   A janela **Regras de monitoramento de operações de arquivos** é exibida.

4. Exportar ou importar regras de monitoramento de operações de arquivos:

- Como exportar as regras de monitoramento de operações de arquivos.

  1. Na parte esquerda da janela **Regras de monitoramento de operações de arquivos**, clique no botão **Exportar**.

     A janela padrão do Microsoft Windows **Salvar como** é exibida.

  2. Especifique o caminho para salvar um arquivo XML com as configurações das regras de monitoramento de operações de arquivos.

  3. Insira o nome do arquivo no campo correspondente.

  4. Clique no botão **Salvar**.

     O aplicativo salvará um arquivo XML com as configurações das regras de monitoramento de operações de arquivos no caminho especificado.

- Como importar as regras para as regras de monitoramento de operações de arquivos.

  1. Na parte esquerda da janela **Regras de monitoramento de operações de arquivos**, clique no botão **Importar**.

  2. No menu de contexto do botão **Importar**, selecione um dos valores:

     - **Mesclar com as regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas não são duplicadas. Se pelo menos uma configuração de regra for exclusiva, a regra será adicionada.
     - **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
     - **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas.

     A janela **Abrir** padrão do Microsoft Windows é exibida.

  3. Especifique o caminho para o arquivo XML com as configurações das regras de monitoramento de acesso ao registro.

  4. Clique no botão **Abrir**.

     As regras importadas serão exibidas na parte esquerda da janela **Regras de monitoramento de operações de arquivos**.

5. Clique no botão **Salvar** para salvar as alterações.

Gerenciamento do Monitor de Integridade de Arquivos por meio do Plug-in da Web

Nesta seção, saiba como configurar a tarefa de Monitor de Integridade de Arquivos por meio do Plug-in da Web.

Configuração da tarefa de Monitor de Integridade de Arquivos

Para definir as configurações da tarefa Monitor de Integridade do Sistema com o uso do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Inspeção do sistema**.
5. Na subseção **Monitor de Integridade de Arquivos**, clique no botão **Configurações**.
   A janela **Monitor de Integridade de Arquivos** é exibida.
6. Na guia **Configurações de monitoramento de operações de arquivos**, defina as seguintes configurações:
   a. Desmarque ou marque a caixa de seleção **Registrar informações sobre operações de arquivos executadas durante o período de interrupção do monitoramento**.

      A caixa de seleção ativa ou desativa o monitoramento das operações do arquivo especificadas nas configurações da tarefa de Monitor de Integridade de Arquivos quando a tarefa não está em execução por alguma razão (remoção de um disco rígido, tarefa interrompida pelo usuário, erro de software).

      Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security for Windows registrará eventos em todos os escopos de monitoramento quando a tarefa Monitor de Integridade de Arquivos não estiver em execução.

      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 marcada por padrão.

   b. Desmarque ou marque a caixa de seleção **Bloquear tentativas de comprometer o log USN**.

      A caixa de seleção ativa ou desativa a proteção do log de USN.

      Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security for Windows bloqueará as tentativas de excluir o log de USN ou comprometer seu conteúdo.

      Se a caixa de seleção estiver desmarcada, o aplicativo não monitorará as alterações do log de USN.

      A caixa de seleção é marcada por padrão.
7. Na guia **Gerenciamento da tarefa** configure a programação de inicialização da tarefa.
8. Clique no botão **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. As informações sobre a data e hora da modificação das configurações são salvas no log de auditoria do sistema.

Criação e configuração de uma regra de monitoramento de operações de arquivos

Para criar e configurar uma regra de monitoramento de operações de arquivos com o uso do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos → Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Inspeção do sistema**.
5. Na subseção **Monitor de Integridade de Arquivos**, clique no botão **Configurações**.

   A janela **Monitor de Integridade de Arquivos** é aberta na guia **Configurações de monitoramento de operações de arquivos**.
6. Clique no botão **Adicionar**.

   A janela **Regra de monitoramento de operações de arquivos** é exibida.
7. Em **Monitorar operações de arquivos para o escopo**, especifique um caminho usando uma das máscaras compatíveis:

   - <*.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 na pasta <\dir>
   - <\dir*\nome.ext> — todos os arquivos com o nome <nome> e a extensão <ext> na pasta <\dir> e todas as subpastas

   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 for Windows não adicionará o escopo de monitoramento especificado.
8. Na guia **Usuários confiáveis**, caso necessário, especifique os usuários confiáveis de uma das seguintes maneiras:

   - Usando o botão **Adicionar**:

     a. Clique no botão **Adicionar**.

     b. Na janela exibida, no campo **Nome do usuário**, especifique o usuário ou grupo de usuários no formato SID.

     c. Clique no botão **OK**.

   - Usando o botão **Adicionar a partir da lista do Servidor de Administração**:

a. Clique no botão **Adicionar a partir da lista do Servidor de Administração**.

b. Na janela exibida, selecione um usuário ou grupo de usuários na lista.

c. Clique no botão **OK**.

Os usuários confiáveis têm permissão para operar arquivos do escopo de monitoramento selecionado.

Por padrão, o Kaspersky Embedded Systems Security for Windows trata todos os usuários que não estejam na lista de usuários confiáveis como não confiáveis e gera eventos críticos para eles. Para usuários confiáveis, as estatísticas são compiladas.

9. Na guia **Marcadores de operações de arquivos**, caso necessário, especifique os marcadores de operações de arquivos que deseja monitorar:

a. Selecione a opção **Detectar operações de arquivo com base nos seguintes marcadores**.

b. Na lista de operações de arquivos disponíveis, selecione as caixas ao lado das operações que deseja monitorar.

Por padrão, o Kaspersky Embedded Systems Security for Windows detecta todos os marcadores de operações de arquivos. A opção **Detectar operações de arquivo com base em todos os marcadores reconhecíveis** está selecionada.

10. Caso queira bloquear todas as operações de arquivos para o escopo de monitoramento selecionado, marque a caixa de seleção **Detectar e bloquear todas as operações de arquivos na área selecionada**.

11. Se quiser que o aplicativo calcule a soma de verificação de um arquivo após ele ter sido modificado:

a. Selecione **Calcular a soma de verificação para o arquivo, se possível. A soma de verificação estará disponível para visualização no relatório da tarefa** relatório de tarefa.

b. Na lista suspensa **Tipo de cálculo de soma de verificação**, selecione uma das opções:

- **Hash SHA256**.
- **Hash MD5**.

12. Caso necessário, adicione pastas ou unidades para excluir as operações de arquivo do monitoramento:

a. Na guia **Exclusões**, marque a caixa de seleção **Excluir as seguintes pastas do controle**.

b. Clique no botão **Adicionar**.

c. Na janela aberta à direita, no campo **Nome da pasta**, insira o caminho para a pasta ou unidade que deseja excluir do escopo de monitoramento de operações de arquivos.

d. Clique no botão **OK**.

O caminho para a pasta ou unidade especificada será exibido na lista.

13. Clique no botão **OK** na janela **Regra de monitoramento de operações de arquivos**.

A regra de monitoramento de operações de arquivos configurada será exibida na janela **Monitor de Integridade do Sistema** na guia **Configurações de monitoramento de operações de arquivos**.

Exportação e importação de regras de monitoramento de operações de arquivos

É possível exportar as regras de monitoramento de operações de arquivos criadas manualmente nas propriedades da tarefa Monitor de Integridade do Sistema para um arquivo XML.

É possível importar as regras de monitoramento de operações de arquivos anteriormente exportadas para um arquivo XML nas propriedades da tarefa Monitor de Integridade do Sistema.

Para exportar ou importar as regras de monitoramento de operações de arquivos com o uso do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Inspeção do sistema**.
5. Na subseção **Monitor de Integridade de Arquivos**, clique no botão **Configurações**.

   A janela **Monitor de Integridade de Arquivos** é aberta na guia **Configurações de monitoramento de operações de arquivos**.
6. Exportar ou importar regras de monitoramento de operações de arquivos:

   - Como exportar as regras de monitoramento de operações de arquivos.

     Clique no botão **Exportar**.

     O aplicativo salva o arquivo FileIntegrityMonitor.xml com as configurações das regras de monitoramento de operações de arquivos na pasta C:\Users\<Nome do usuário>\Downloads.

   - Como importar as regras para as regras de monitoramento de operações de arquivos.

1. Clique no botão **Importar**.

   A janela **Abrir** padrão do Microsoft Windows é exibida.

2. Especifique o caminho para o arquivo XML com as configurações das regras de monitoramento de operações de arquivos.

3. Clique no botão **Abrir**.

   As regras importadas via mesclagem da lista de regras serão exibidas na janela **Monitor de Integridade de Arquivos** na guia **Configurações de monitoramento de operações de arquivos**.

   Caso as configurações da regra do Monitor de Integridade do Sistema da lista de regras importadas sejam idênticas às configurações da regra já existente, essa regra não será adicionada da lista de regras importadas.

7. Clique no botão **OK** para salvar as alterações.

Scanner AMSI

Esta seção contém informações sobre a tarefa AMSI scanner e como configurá-la.

Sobre a tarefa AMSI Scanner

Quando a tarefa AMSI scanner está em execução, o Kaspersky Embedded Systems Security for Windows controla a execução de scripts criados usando as tecnologias de script do Microsoft Windows (Active Scripting), como VBScript ou JScript®. O aplicativo também pode processar scripts do PowerShell™ e scripts executados nos aplicativos do Microsoft Office em sistemas operacionais com a Interface de Verificação Antimalware (AMSI) instalada. É possível permitir ou bloquear a execução de um script que foi considerado perigoso ou provavelmente perigoso. Caso o Kaspersky Embedded Systems Security for Windows identifique um script como potencialmente perigoso, ele bloqueia ou permite a sua execução de acordo com a ação selecionada. Caso a ação **Bloquear** seja selecionada, o aplicativo permitirá a execução de script apenas se um script for considerado seguro.

A partir do sistema operacional Microsoft Windows 10 e Microsoft Windows Server 2016, o Kaspersky Embedded Systems Security for Windows será compatível com a Interface de Verificação Antimalware (AMSI). O AMSI permite que aplicativos e serviços se integrem a qualquer aplicativo antimalware instalado em um dispositivo para que todos os scripts executados sejam interceptados e verificados pelo antimalware.

É possível encontrar mais informações sobre a funcionalidade AMSI no site do Microsoft Windows.

É possível definir as configurações da tarefa AMSI scanner.

Configurações padrão da tarefa do AMSI Scanner

A tarefa do sistema local AMSI scanner usa as configurações padrão descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Configurações padrão da tarefa do AMSI scanner

Configuração	Valor padrão	Descrição
Ação a ser executada em scripts perigosos	**Bloquear**	É possível especificar a ação a ser executada ao detectar scripts provavelmente perigosos: bloquear ou permitir a execução.
Analisador heurístico	O nível de segurança **Médio** é aplicado.	O analisador heurístico pode ser ativado ou desativado. O nível de análise pode ser configurado.
Zona confiável	Usada	Lista geral de exclusões que podem ser usadas em tarefas selecionadas.

Definindo as configurações da tarefa do AMSI Scanner por meio do Plugin de Administração

Para configurar uma tarefa do AMSI scanner, faça o seguinte:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Proteção do servidor em tempo real** da janela **Propriedades: <nome da política>**, clique em **Configurações** para o **AMSI scanner**.

5. Na seção **Ação a ser executada em scripts perigosos**, na guia **Geral**, execute uma das seguintes ações:

   - Para permitir a execução de scripts provavelmente perigosos, selecione **Permitir**.

   - Para bloquear a execução de scripts provavelmente perigosos, selecione **Bloquear**.

6. Na seção **Analisador heurístico**, execute uma das seguintes ações:

   - Desmarque ou marque a caixa de seleção **Usar o Analisador heurístico**.

   - Se necessário, ajuste o nível da análise usando o controle deslizante.

7. Na seção **Zona confiável**, marque ou desmarque a caixa de seleção **Aplicar Zona Confiável**.

8. Clique no botão **OK**.

As configurações recém-definidas são aplicadas.

Definindo as configurações da tarefa do AMSI Scanner por meio do Console do Aplicativo

Para configurar uma tarefa do AMSI scanner, faça o seguinte:

1. Na árvore do Console do Aplicativo, expanda o node **Proteção do Computador em Tempo Real**.

2. Selecione o node secundário do **AMSI scanner**.

3. Clique no link **Propriedades** no painel de resultados do node.

   A janela **Configurações de tarefa** é exibida na guia **Geral**.

4. Na seção **Ação a ser executada em scripts perigosos**, execute uma das seguintes ações:

   - Para permitir a execução de scripts provavelmente perigosos, selecione **Permitir**.

   - Para bloquear a execução de scripts provavelmente perigosos, selecione **Bloquear**.

5. Na seção **Analisador heurístico**, execute uma das seguintes ações:

   - Desmarque ou marque a caixa de seleção **Usar o Analisador heurístico**.

   - Se necessário, ajuste o nível da análise usando o controle deslizante.

6. Na seção **Zona confiável**, marque ou desmarque a caixa de seleção **Aplicar Zona Confiável**.
7. Clique no botão **OK**.

As configurações recém-definidas são aplicadas.

Definindo as configurações da tarefa do AMSI Scanner por meio do Plugin da Web

Para configurar uma tarefa do AMSI scanner, faça o seguinte:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Proteção do Servidor em Tempo Real**.
5. Clique em **Configurações** na subseção **AMSI scanner**.
6. Na seção **Ação a ser executada em scripts perigosos**, na guia **Geral**, execute uma das seguintes ações:
   - Para permitir a execução de scripts provavelmente perigosos, selecione **Permitir**.
   - Para bloquear a execução de scripts provavelmente perigosos, selecione **Bloquear**.
7. Na seção **Analisador heurístico**, execute uma das seguintes ações:
   - Desmarque ou marque a caixa de seleção **Usar o Analisador heurístico**.
   - Caso seja necessário, ajuste o nível da análise heurística.
8. Na seção **Zona confiável**, marque ou desmarque a caixa de seleção **Aplicar Zona Confiável**.
9. Clique no botão **OK**.

As configurações recém-definidas são aplicadas.

Estatísticas da tarefa do AMSI Scanner

Enquanto a tarefa **AMSI scanner** está em execução, é possível visualizar as informações sobre o número de scripts processados pelo Kaspersky Embedded Systems Security for Windows desde o momento em que a tarefa foi iniciada.

Para visualizar as estatísticas de tarefas do AMSI scanner, faça o seguinte:

1. Na árvore do Console do Aplicativo, expanda o node **Proteção do Computador em Tempo Real**.
2. Selecione o node secundário do **AMSI scanner**.

As estatísticas de tarefas atuais são exibidas no painel de resultados do node nas seções **Gerenciamento** e **Estatísticas**.

É possível visualizar as informações sobre os objetos processados pelo Kaspersky Embedded Systems Security for Windows desde quando a tarefa foi iniciada (consulte a tabela abaixo).

Estatísticas da tarefa do AMSI Scanner

Campo	Descrição
Scripts bloqueados	Número total de scripts bloqueados pelo Kaspersky Embedded Systems Security for Windows.
Scripts perigosos detectados	Número de scripts perigosos detectados.
Scripts possivelmente perigosos detectados	Número de scripts provavelmente perigosos detectados.
Scripts processados	Número total de scripts processados.

Monitor de acesso ao registro

Esta seção explica como iniciar e configurar a tarefa do Monitor de acesso ao registro.

Sobre a tarefa do Monitor de Acesso ao Registro

A tarefa de Monitor de acesso ao registro foi desenvolvida para rastrear as ações executadas com as ramificações e chaves de registro especificadas nos escopos de monitoramento definidos nas configurações de tarefas. A tarefa rastreia as ações no sistema operacional instalado no dispositivo ou nos contêineres do Windows Server 2016 e definidos posteriormente no escopo de monitoramento. É possível utilizar a tarefa para detectar as alterações que indicam uma violação de segurança no dispositivo protegido.

Para iniciar a tarefa Monitor de acesso ao registro, é necessário configurar pelo menos uma regra de monitoramento.

Sobre as regras de monitoramento de acesso ao registro

A tarefa **Monitor de acesso ao registro** é executada de acordo com as regras de monitoramento de acesso ao registro. É possível utilizar os critérios para acionamento de regras para configurar as condições que acionam a tarefa e definir o nível de importância de eventos detectados e registrados no log de tarefas.

Uma regra do monitor de acesso ao registro é especificada para cada escopo de monitoramento.

É possível configurar os seguintes critérios para acionamento de regras:

- **Ações**
- **Valores controlados**
- **Usuários confiáveis**

Ações

Quando a tarefa Monitor de acesso ao registro é iniciada, o Kaspersky Embedded Systems Security for Windows utiliza uma lista de ações para monitorar o registro (veja a tabela abaixo).

Caso uma ação especificada como um critério para acionamento de regras seja detectada, o aplicativo registra um log de evento correspondente.

O nível de importância dos eventos registrados em log não depende das ações selecionadas ou do número de eventos.

Por padrão, o Kaspersky Embedded Systems Security for Windows considera todas as ações. É possível configurar a lista de ações manualmente nas configurações de regra da tarefa.

Ações

Ação	Restrições	Sistema operacional
Criar a chave	• Para Windows XP e Windows Server 2003, caso adicione **Ações** à lista de **Criar a chave** e, em seguida, selecione o modo **Bloquear operações de acordo com as regras**, a criação da chave não é bloqueada nos sistemas operacionais especificados devido às restrições do sistema. A chave é criada com a respectiva notificação enviada para o log de eventos. • Caso queira proibir a criação de uma chave específica por meio do Editor de Registro, crie uma regra para uma chave de registro pai e certifique-se de adicionar **Ações** à lista de **Criar subchaves** e, em seguida, selecione o modo **Bloquear operações de acordo com as regras**.	Windows XP e posterior
Excluir a chave	Caso queira excluir uma chave principal, desmarque as opções **Excluir subchaves** e **Ações** na lista de **Excluir a chave** monitoradas para uma chave de registro configurada, pois só é possível excluir a chave principal com subchaves.	Windows XP e posterior
Renomear a chave	N/A	Windows XP e posterior
Alterar as configurações de segurança da chave	N/A	Windows Vista e posterior
Excluir os valores	N/A	Windows XP e posterior
Definir os valores	Caso queira adicionar **Ações** na lista de **Definir os valores**, definir o **Valor ou máscara de valor** padrão na regra para uma chave e, a seguir, selecionar **Bloquear operações de acordo com as regras**, a chave não será criada, porque uma nova chave só pode ser criada com um valor padrão.	Windows XP e posterior
Criar subchaves	N/A	Windows XP e posterior
Excluir subchaves	N/A	Windows XP e posterior
Renomear subchaves	N/A	Windows XP e posterior
Alterar as configurações de segurança das subchaves	N/A	Windows Vista e posterior

Valores de registro

Além do monitoramento das chaves de registro, é possível bloquear ou monitorar as alterações dos valores do registro existentes. As seguintes opções estão disponíveis:

- **Definir o valor** - criar os novos valores de registro ou alterar os valores de registro existentes.
- **Excluir o valor** - excluir os valores de registro existentes.

A renomeação e a alteração das configurações de segurança não se aplicam aos valores do registro.

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 do evento criando uma lista de usuários confiáveis nas configurações da regra de monitoramento do registro do sistema.

Usuário não confiável é qualquer usuário não indicado na lista de usuário confiável nas configurações da regra de escopo de monitoramento. Caso o Kaspersky Embedded Systems Security for Windows detecte uma ação realizada por um usuário não confiável, a tarefa Monitor de acesso ao registro registra um evento crítico no log de tarefas.

Usuário confiável é um usuário ou grupo de usuários autorizados a realizar ações dentro do escopo de monitoramento especificado. Caso o Kaspersky Embedded Systems Security for Windows detecte uma ação realizada por um usuário confiável, a tarefa de Monitor de Acesso ao Registro registrará um evento informativo no log de tarefas.

Configurações padrão da tarefa do Monitor de acesso ao registro

As configurações padrão para a tarefa Monitor de acesso ao registro são descritas na tabela abaixo. É possível alterar os valores das configurações nos seguintes componentes:

- O Plug-in de Administração
- O Console do Aplicativo
- O Plug-in da Web

Configurações padrão da tarefa do Monitor de acesso ao registro

Configuração	Valor padrão	Descrição
Escopo de monitoramento	Não definido	Use essa opção para definir as chaves e subchaves de registro pai a serem monitoradas. A configuração é obrigatória. Caso a configuração não seja definida, a tarefa falhará ao iniciar. Os eventos de monitoramento são gerados para as chaves e subchaves de registro pai no escopo de monitoramento especificado.
Ações	Todos os itens da lista de ações são selecionados	Use essa opção para configurar uma lista de ações conforme aplicável marcando e desmarcando as respectivas caixas de seleção.
Valores de registro	Não definido	Use essa opção para adicionar, modificar e remover os valores do registro que deseja monitorar para o escopo de monitoramento definido.
Usuários confiáveis	Não definido	É possível especificar os usuários e grupos de usuários autorizados a executar as ações definidas para as chaves de registro especificadas.

Modo da tarefa.	Somente estatísticas	É possível selecionar o modo de tarefa para **Bloquear operações de acordo com as regras** ou selecionar o modo **Somente estatísticas** para receber as notificações.
Programação de inicialização da tarefa	Não definido	É possível definir as configurações para iniciar a tarefa de acordo com a programação.

Gerenciamento do Monitor de acesso ao registro por meio do Plug-in de Administração

Nesta seção, saiba como configurar a tarefa Monitor de acesso ao registro por meio do plug-in de administração.

Definição das configurações da tarefa do Monitor de acesso ao registro

Para definir as configurações da tarefa Monitor de Acesso ao Registro usando o Plug-in de Administração:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Inspeção do sistema**, no bloco **Monitor de acesso ao registro**, clique no botão **Configurações**.

   A janela de **Monitor de acesso ao registro** é exibida.
5. Na guia **Configurações do monitor de acesso ao registro**, no bloco **Modo da tarefa**, selecione a opção necessária na lista:
   - **Bloquear operações de acordo com as regras**

     Caso selecione o modo **Bloquear as operações de acordo com as regras**, o Kaspersky Embedded Systems Security for Windows bloqueia as **Ações** definidas para o escopo de monitoramento.

     Por padrão, o modo **Somente Estatísticas** é aplicado.
   - **Somente estatísticas**.

Caso o modo **Somente Estatísticas** esteja selecionado para o escopo de monitoramento, o Kaspersky Embedded Systems Security for Windows compila as estatísticas das ações da chave de registro de acordo com as regras configuradas.

Por padrão, o modo **Somente Estatísticas** é aplicado.

6. Adicione regras de monitoramento de acesso ao registro que determinarão o que a tarefa fará.
7. Na guia **Gerenciamento da tarefa** defina as configurações de programação de inicialização da tarefa.
8. Clique no botão **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. As informações sobre a data e hora da modificação das configurações são salvas no log de auditoria do sistema.

Criação e configuração de uma regra de monitoramento de acesso ao registro

As regras de monitoramento de acesso ao registro são aplicadas na ordem em que estão listadas no bloco **Regras do monitor de acesso ao registro**.

Para criar e configurar uma regra do monitor de acesso ao registro usando o Plug-in de Administração:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Execute uma das seguintes ações:
   - Caso esteja criando uma regra do monitor de acesso ao registro em uma política, na seção **Inspeção do sistema**, no bloco **Monitor de acesso ao registro**, clique no botão **Configurações**.

     A janela **Monitor de acesso ao registro** é aberta na guia **Configurações do monitor de acesso ao registro**.
   - Caso esteja criando uma regra do monitor de acesso ao registro para uma tarefa local, na janela **Propriedades: Monitor de Acesso ao Registro**, vá para a seção **Configurações**.
5. No bloco **Regras do monitor de acesso ao registro**, clique no botão **Adicionar**.

   A janela **Regra do monitor de acesso ao registro** é exibida.
6. No campo **Definir os critérios de acionamento de regra para o escopo especificado**, insira o caminho com o uso de uma **máscara compatível**.

É possível utilizar `?` e `*` como uma máscara ao inserir em um caminho.

Caso o caminho para uma chave de registro raiz seja inserido, certifique-se de especificar o caminho completo sem uma máscara, como `HKEY_USERS`. A seguir está uma lista de chaves de registro raiz válidas:

- `HKEY_LOCAL_MACHINE`
- `HKLM`
- `HKEY_CURRENT_USER`
- `HKCU`
- `HKEY_USERS`
- `HKUS`
- `HKU`
- `HKEY_CURRENT_CONFIG`
- `HKEY_CLASSES_ROOT`
- `HKCR`

Evite usar máscaras com suporte para as chaves raiz ao criar as regras.
Se for especificado apenas uma chave raiz, como HKEY_CURRENT_USER, ou uma chave raiz com uma máscara para todas as chaves secundárias, como HKEY_CURRENT_USER*, um grande número de notificações sobre o endereçamento das chaves secundárias especificadas serão geradas, o que resultará em problemas de desempenho do sistema. Se for especificada uma chave raiz, como HKEY_CURRENT_USER, ou uma chave raiz com uma máscara para todas as chaves secundárias, como HKEY_CURRENT_USER*, e selecionado o modo **Bloquear operações de acordo com as regras**, o sistema não será capaz de ler ou alterar o necessárias para o funcionamento do sistema operacional e falhará na resposta.

7. Na guia **Adicionar**, configure a lista de ações conforme for necessário.

8. Especifique os valores do registro que a regra monitorará:

   a. Na guia **Valores de registro**, clique no botão **Adicionar**.

      A janela **Regra de valor do registro** é exibida.

   b. No campo correspondente, insira uma máscara de valor do registro.

   c. No bloco **Operações controladas**, selecione quais ações executadas no valor do registro serão monitoradas pela regra.

   d. Clique no botão **OK** para salvar as alterações.

9. Caso necessário, especifique os usuários confiáveis:

a. Na guia **Usuários confiáveis**, no menu de contexto do botão **Adicionar**, selecione o método para adicionar usuários confiáveis.

A janela **Seleção de usuário ou grupo de usuários** é aberta.

b. Selecione um usuário ou grupo de usuários que tenha permissão para executar as ações selecionadas.

c. Clique no botão **OK** para salvar as alterações.

Por padrão, o Kaspersky Embedded Systems Security for Windows trata todos os usuários que não estejam na lista de usuários confiáveis como não confiáveis e gera eventos críticos para eles. Para usuários confiáveis, as estatísticas são compiladas.

10. Na janela **Regra do monitor de acesso ao registro**, clique no botão **OK**.

A regra de monitoramento de acesso ao registro configurada é exibida na janela **Monitor de acesso ao registro / Propriedades: Monitor de Acesso ao Registro** no bloco **Regras do monitor de acesso ao registro**.

Exportação e importação de regras de monitoramento de acesso ao registro

É possível exportar as regras de monitoramento de acesso ao registro criadas manualmente nas propriedades da tarefa Monitor de Acesso ao Registro para um arquivo XML.

É possível importar as regras de monitoramento de acesso ao registro anteriormente exportadas para um arquivo XML nas propriedades da tarefa Monitor de Acesso ao Registro.

Para exportar ou importar as regras de monitoramento de acesso ao registro com o uso do Plug-in de Administração:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Execute uma das seguintes ações:

   - Caso queira importar ou exportar regras para monitorar o acesso ao registro em uma política, na seção **Inspeção do sistema**, no bloco **Monitor de acesso ao registro**, clique no botão **Configurações**.

     A janela **Monitor de acesso ao registro** é aberta na guia **Configurações do monitor de acesso ao registro**.

   - Caso queira importar ou exportar as regras de monitoramento de acesso ao registro para uma tarefa local, na janela **Propriedades: Monitor de Acesso ao Registro**, vá para a seção **Configurações**.

5. Exportação ou importação das regras de monitoramento de acesso ao registro:

- Como exportar as regras de monitoramento de acesso ao registro.

  1. No bloco **Regras do monitor de acesso ao registro**, clique no botão **Exportar**.

     A janela padrão do Microsoft Windows **Salvar como** é exibida.

  2. Especifique o caminho para salvar o arquivo XML com as configurações das regras de monitoramento de acesso ao registro.

  3. Insira o nome do arquivo no campo correspondente.

  4. Clique no botão **Salvar**.

     O aplicativo salvará um arquivo XML com as configurações das regras de monitoramento de acesso ao registro no caminho especificado.

- Como importar as regras de monitoramento de acesso ao registro.

  1. No bloco **Regras do monitor de acesso ao registro**, clique no botão **Importar**.

  2. No menu de contexto do botão **Importar**, selecione um dos valores:

     - **Mesclar com as regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes.

       Caso o nome da ramificação do registro na regra importada corresponda ao nome da ramificação do registro de uma regra existente, a regra importada não será adicionada, mesmo que os valores das configurações dessa ramificação do registro sejam diferentes nas regras.

     - **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.

     - **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas.

     A janela **Abrir** padrão do Microsoft Windows é exibida.

  3. Especifique o caminho para o arquivo XML com as configurações das regras de monitoramento de acesso ao registro.

  4. Clique no botão **Abrir**.

     Na janela **Monitor de Acesso ao Registro / Propriedades: Monitor de Acesso ao Registro**, as regras importadas serão exibidas na seção **Regras do monitor de acesso ao registro**.

6. Clique no botão **Salvar** para salvar as alterações.

Gerenciamento da tarefa do Monitor de Acesso ao Registro por meio do Console do Aplicativo

Nesta seção, saiba como configurar a tarefa do Monitor de acesso ao registro por meio do Console de Aplicação.

Definição das configurações gerais da tarefa do Monitor de Acesso ao Registro

Para definir as configurações gerais da tarefa Monitor de Acesso ao Registro por meio do Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o node **Inspeção do sistema**.
2. Selecione o node secundário do **Monitor de acesso ao registro**.
3. Clique no link **Propriedades** no painel de resultados do node do **Monitor de acesso ao registro**.
   A janela **Configurações de tarefa** é exibida na guia **Geral**.
4. No bloco **Modo da tarefa**, selecione a opção necessária na lista:
   - **Bloquear operações de acordo com as regras**

     Caso selecione o modo **Bloquear as operações de acordo com as regras**, o Kaspersky Embedded Systems Security for Windows bloqueia as **Ações** definidas para o escopo de monitoramento.

     Por padrão, o modo **Somente Estatísticas** é aplicado.

   - **Somente estatísticas**.

     Caso o modo **Somente Estatísticas** esteja selecionado para o escopo de monitoramento, o Kaspersky Embedded Systems Security for Windows compila as estatísticas das ações da chave de registro de acordo com as regras configuradas.

     Por padrão, o modo **Somente Estatísticas** é aplicado.
5. Nas guias **Agendamento** e **Avançado**, configure a programação de inicialização da tarefa.
6. Clique no botão **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. As informações sobre a data e hora da modificação das configurações são salvas no log de auditoria do sistema.

Criação e configuração de uma regra de monitoramento de acesso ao registro

As regras de monitoramento de acesso ao registro são aplicadas na ordem em que estão listadas no bloco **Regras do monitor de acesso ao registro**.

Para criar e configurar uma regra de monitoramento de acesso ao registro usando o Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o node **Inspeção do sistema**.

2. Selecione o node secundário do **Monitor de acesso ao registro**.

3. Clique no link **Monitor de acesso ao registro** no painel de resultados do node do **Regras do monitor de acesso ao registro**.

   A janela de **Monitor de acesso ao registro** é exibida.

4. No campo **Adicione a chave de registro do sistema para monitorar**, insira o caminho para a chave do registro usando uma máscara compatível.

   Evite usar máscaras compatíveis para as chaves raiz ao criar as regras.
   Caso apenas uma chave raiz seja especificada, como HKEY_CURRENT_USER, ou uma chave raiz com uma máscara para todas as chaves secundárias, como HKEY_CURRENT_USER*, um grande número de notificações sobre como abordar as chaves secundárias especificadas será gerado, o que resulta em problemas de desempenho do sistema.
   Se você especificar uma chave raiz, como HKEY_CURRENT_USER, ou uma chave raiz com uma máscara para todas as chaves secundárias, como HKEY_CURRENT_USER*, e selecionar o modo **Bloquear operações de acordo com as regras**, o sistema não poderá ler ou alterar as chaves necessárias para o funcionamento do sistema operacional e não responderá.

5. Clique no botão **Adicionar**.

6. Na guia **Ações** da área de escopo de monitoramento selecionada, configure a lista de ações conforme o necessário.

7. Especifique os valores do registro que a regra monitorará:

   a. Na guia **Valores controlados**, clique no botão **Adicionar**.

      A janela **Regra de valor do registro** é exibida.

   b. No campo correspondente, insira o valor do registro ou a máscara do valor do registro.

   c. No bloco **Operações controladas**, selecione quais ações executadas no valor do registro serão monitoradas pela regra.

   d. Clique no botão **OK** para salvar as alterações.

8. Caso necessário, especifique os usuários confiáveis:

   a. Na guia **Usuários confiáveis**, clique no botão **Adicionar**.

   b. Na janela **Selecionar Usuários ou Grupos**, selecione os usuários ou grupos de usuários autorizados a executar as ações selecionadas.

   c. Clique no botão **OK** para salvar as alterações.

   Por padrão, o Kaspersky Embedded Systems Security for Windows trata todos os usuários que não estejam na lista de usuários confiáveis como não confiáveis e gera eventos críticos para eles. Para usuários confiáveis, as estatísticas são compiladas.

9. Na janela **Monitor de acesso ao registro**, clique no botão **Salvar**.

A regra de monitoramento de acesso ao registro configurada é exibida no bloco **Monitor de acesso ao registro** da janela **Regras do monitor de acesso ao registro**.

Exportação e importação de regras de monitoramento de acesso ao registro

É possível exportar as regras de monitoramento de acesso ao registro criadas manualmente nas propriedades da tarefa Monitor de Acesso ao Registro para um arquivo XML.

É possível importar as regras de monitoramento de acesso ao registro anteriormente exportadas para um arquivo XML nas propriedades da tarefa Monitor de Acesso ao Registro.

Para exportar e importar as regras de monitoramento de acesso ao registro usando o Console do Aplicativo:

1. Na árvore do Console do Aplicativo, expanda o node **Inspeção do sistema**.
2. Selecione o node secundário do **Monitor de acesso ao registro**.
3. Clique no link **Monitor de acesso ao registro** no painel de resultados do node do **Regras do monitor de acesso ao registro**.

   A janela de **Monitor de acesso ao registro** é exibida.
4. Como exportar as regras de monitoramento de acesso ao registro.

   1. No bloco **Regras do monitor de acesso ao registro**, clique no botão **Exportar para um arquivo** para exportar as regras de monitoramento de acesso ao registro.

      A janela padrão do Microsoft Windows **Salvar como** é exibida.
   2. Especifique o caminho para salvar o arquivo XML com as configurações das regras de monitoramento de acesso ao registro.
   3. Insira o nome do arquivo no campo correspondente.
   4. Clique no botão **Salvar**.

      O aplicativo salvará um arquivo XML com as configurações das regras de monitoramento de acesso ao registro no caminho especificado.
5. Como importar as regras de monitoramento de acesso ao registro.

1. No bloco **Regras do monitor de acesso ao registro**, clique no botão **Importar**.
2. No menu de contexto do botão **Importar**, selecione um dos valores:
   - **Mesclar com as regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes.

     Caso o nome da ramificação do registro na regra importada corresponda ao nome da ramificação do registro de uma regra existente, a regra importada não será adicionada, mesmo que os valores das configurações dessa ramificação do registro sejam diferentes nas regras.

   - **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
   - **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas.

   A janela **Abrir** padrão do Microsoft Windows é exibida.
3. Especifique o caminho para o arquivo XML com as configurações das regras de monitoramento de acesso ao registro.
4. Clique no botão **Abrir**.

   As regras importadas serão exibidas no bloco **Monitor de acesso ao registro** da janela **Regras do monitor de acesso ao registro**.

6. Clique no botão **Salvar** para salvar as alterações.

Gerenciamento do Monitor de acesso ao registro por meio do plug-in da Web

Nesta seção, saiba como configurar a tarefa do Monitor de acesso ao registro por meio do plug-in da Web.

Definição das configurações da tarefa do Monitor de acesso ao registro

Para configurar a tarefa do Monitor de acesso ao registro por meio do plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Inspeção do sistema**.
5. Na subseção **Monitor de acesso ao registro**, clique no botão **Configurações**.

A janela **Monitor de acesso ao registro** é aberta na guia **Configurações do monitor de acesso ao registro**.

6. No bloco **Modo da tarefa**, selecione a opção necessária pela lista:

   - **Bloquear operações de acordo com as regras**

     Caso selecione o modo **Bloquear as operações de acordo com as regras**, o Kaspersky Embedded Systems Security for Windows bloqueia as **Ações** definidas para o escopo de monitoramento.

     Por padrão, o modo **Somente Estatísticas** é aplicado.

   - **Somente estatísticas**

     Caso o modo **Somente Estatísticas** esteja selecionado para o escopo de monitoramento, o Kaspersky Embedded Systems Security for Windows compila as estatísticas das ações da chave de registro de acordo com as regras configuradas.

     Por padrão, o modo **Somente Estatísticas** é aplicado.

7. Adicione regras de monitoramento de acesso ao registro que determinarão o que a tarefa fará.

8. Na guia **Gerenciamento da tarefa** configure a programação de inicialização da tarefa.

9. Clique no botão **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security for Windows aplica as novas configurações à tarefa em execução. As informações sobre a data e hora da modificação das configurações são salvas no log de auditoria do sistema.

Criação e configuração de uma regra de monitoramento de acesso ao registro

As regras de monitoramento de acesso ao registro são aplicadas na ordem em que estão listadas no bloco **Regras do monitor de acesso ao registro**.

Para criar e configurar uma regra de monitoramento de acesso ao registro com o uso do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.

2. Clique no nome da política que você quer configurar.

3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.

4. Selecione a seção **Inspeção do sistema**.

5. Na subseção **Monitor de acesso ao registro**, clique no botão **Configurações**.

   A janela **Monitor de acesso ao registro** é aberta na guia **Configurações do monitor de acesso ao registro**.

6. No bloco **Regras do monitor de acesso ao registro**, clique no botão **Adicionar**.

   A janela **Regra do monitor de acesso ao registro** é exibida.

7. No campo **Monitorar o acesso ao registro para um escopo**, insira um caminho com o uso de uma **máscara compatível**.

   É possível utilizar `?` e `*` como uma máscara ao inserir em um caminho.

   Caso o caminho para uma chave de registro raiz seja inserido, certifique-se de especificar o caminho completo sem uma máscara, como `HKEY_USERS`. A seguir está uma lista de chaves de registro raiz válidas:

   - `HKEY_LOCAL_MACHINE`
   - `HKLM`
   - `HKEY_CURRENT_USER`
   - `HKCU`
   - `HKEY_USERS`
   - `HKUS`
   - `HKU`
   - `HKEY_CURRENT_CONFIG`
   - `HKEY_CLASSES_ROOT`
   - `HKCR`

   Evite usar máscaras compatíveis para as chaves raiz ao criar as regras.
   Caso apenas uma chave raiz seja especificada, como HKEY_CURRENT_USER, ou uma chave raiz com uma máscara para todas as chaves secundárias, como HKEY_CURRENT_USER*, um grande número de notificações sobre como abordar as chaves secundárias especificadas será gerado, o que resulta em problemas de desempenho do sistema.
   Se você especificar uma chave raiz, como HKEY_CURRENT_USER, ou uma chave raiz com uma máscara para todas as chaves secundárias, como HKEY_CURRENT_USER*, e selecionar o modo **Bloquear operações de acordo com as regras**, o sistema não poderá ler ou alterar as chaves necessárias para o funcionamento do sistema operacional e não responderá.

8. Na guia **Ações** da área de escopo de monitoramento selecionada, configure a lista de ações conforme o necessário.

9. Especifique os valores do registro que a regra monitorará:

   a. Na guia **Valores controlados**, clique no botão **Adicionar**.

      A janela **Regra de valor do registro** é exibida.

   b. No campo correspondente, insira uma máscara de valor do registro.

   c. No bloco **Operações controladas**, selecione quais ações executadas com o valor do registro serão monitoradas pela regra.

   d. Clique no botão **OK** para salvar as alterações.

10. Caso necessário, especifique os usuários confiáveis:

    a. Na guia **Usuários confiáveis**, clique no botão **Adicionar**.

    b. Insira o **Nome do usuário** ou clique em **Definir SID para o grupo Todos** para definir os usuários autorizados a executar as ações selecionadas.

    c. Clique no botão **OK** para salvar as alterações.

    Por padrão, o Kaspersky Embedded Systems Security for Windows trata todos os usuários que não estejam na lista de usuários confiáveis como não confiáveis e gera eventos críticos para eles. Para usuários confiáveis, as estatísticas são compiladas.

11. Na janela **Regra do monitor de acesso ao registro**, clique no botão **OK** para salvar as alterações.

A regra de monitoramento de acesso ao registro configurada é exibida no bloco **Monitor de acesso ao registro** da janela **Regras do monitor de acesso ao registro**.

Exportação e importação de regras de monitoramento de acesso ao registro

É possível exportar as regras de monitoramento de acesso ao registro criadas manualmente nas propriedades da tarefa Monitor de Acesso ao Registro para um arquivo XML.

É possível importar as regras de monitoramento de acesso ao registro anteriormente exportadas para um arquivo XML nas propriedades da tarefa Monitor de Acesso ao Registro.

Para exportar ou importar as regras de monitoramento de acesso ao registro com o uso do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Inspeção do sistema**.
5. No bloco **Monitor de acesso ao registro**, clique no botão **Configurações**.
   A janela **Monitor de acesso ao registro** é aberta na guia **Configurações do monitor de acesso ao registro**.
6. Exportação ou importação das regras de monitoramento de acesso ao registro:

   - Como exportar as regras de monitoramento de acesso ao registro.

     No bloco **Regras do monitor de acesso ao registro**, clique no botão **Exportar**.

     O aplicativo salva o arquivo RegistryMonitor.xml com as configurações das regras de monitoramento de acesso ao registro na pasta C:\Users\<Nome do usuário>\Downloads.

   - Como importar as regras de monitoramento de acesso ao registro.

1. No bloco **Regras do monitor de acesso ao registro**, clique no botão **Importar**.
2. Clique no botão **Importar**.

   A janela **Abrir** padrão do Microsoft Windows é exibida.
3. Especifique o caminho para o arquivo XML com as configurações das regras de monitoramento de acesso ao registro.
4. Clique no botão **Abrir**.

   As regras importadas via mesclagem da lista de regras serão exibidas no bloco **Monitor de acesso ao registro** da janela **Regras do monitor de acesso ao registro**.

   Caso o nome da ramificação do registro na regra importada corresponda ao nome da ramificação do registro de uma regra existente, a regra importada não será adicionada, mesmo que os valores das configurações dessa ramificação do registro sejam diferentes nas regras.

7. Clique no botão **Salvar** para salvar as alterações.

Inspeção do Log

Esta seção contém informações sobre a tarefa de Inspeção do Log e definição de configurações de tarefa.

Sobre a tarefa de Inspeção do Log

Quando a tarefa de Inspeção do Log é executada, o Kaspersky Embedded Systems Security for Windows, monitora a integridade do ambiente protegido com base nos resultados de uma inspeção dos logs de eventos do Windows. O aplicativo notifica o administrador ao detectar um comportamento anormal que pode indicar tentativas de ataques cibernéticos.

O Kaspersky Embedded Systems Security for Windows analisa os logs de eventos do Windows e identifica violações com base nas regras especificadas pelo usuário ou pelas configurações do analisador heurístico, que a tarefa usa para inspecionar logs.

Regras predefinidas e análise heurística

É possível utilizar a tarefa de Inspeção do Log para monitorar o estado do sistema protegido aplicando regras predefinidas com base na heurística existente. O analisador heurístico identifica atividade anormal no dispositivo 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. É possível ativar ou desativar qualquer uma dessas regras. Não é possível excluir regras existentes ou criar novas regras.

É possível configurar critérios para 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 for Windows 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

É possível usar configurações de regra 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 de Inspeção do Log contém quatro regras. É possível ativar e desativar essas 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 na regra. Também é possível adicionar e remover identificadores para cada regra especificada.

- Fonte de evento.

  Para cada regra, é possível especificar um log dentro do Log de Eventos do Windows. O aplicativo procurará registros com os identificadores de evento especificados apenas nesse log. É possível selecionar um dos logs padrão (Aplicativo, Segurança ou Sistema), ou especificar um log personalizado digitando o nome no campo de seleção de fonte.

  O aplicativo não verifica se o log especificado realmente existe no Log de Eventos do Windows.

Quando a regra é acionada, o Kaspersky Embedded Systems Security for Windows registra um Evento crítico no log de tarefas de Inspeção do Log.

Por padrão, a tarefa de Inspeção do Log 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 para obter detalhes.

Configurações padrão da tarefa de Inspeção do Log

Por padrão, a tarefa de Inspeção do Log possui as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Configurações padrão da tarefa de Inspeção do Log

Configuração	Valor padrão	Descrição
Aplicar regras personalizadas para inspeção do log	Não aplicado.	Você pode ativar, desativar, adicionar ou alterar as regras personalizadas.
Aplicar regras predefinidas para inspeção do log	Aplicada.	É possível ativar ou desativar o analisador heurístico, que detecta atividades anormais no dispositivo protegido.
Detecção de ataque de força bruta	10 falhas de login por 300 segundos.	É possível definir o número de tentativas e o período, que serão considerados como acionadores pelo analisador heurístico.
Login da rede	0:00:00.	É possível indicar o início e o fim do intervalo de tempo durante o qual o Kaspersky Embedded Systems Security for Windows encara tentativas de conexão como atividades anormais.
Exclusões	Não aplicado.	É possível especificar usuários e endereços IP que não acionarão o analisador heurístico.
Programação de inicialização da tarefa	A primeira execução não está programada.	É possível definir configurações para a inicialização programada da tarefa.

Gerenciamento das regras de Inspeção do Log por meio do Plug-in de Administração

Nesta seção, saiba como adicionar e configurar regras de Inspeção do Log por meio do Plug-in de Administração.

Configuração de regras de tarefa predefinidas

Realize as seguintes ações para configurar regras predefinidas para a tarefa de Inspeção do Log:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.
4. Na seção **Inspeção do sistema**, clique no botão **Inspeção do Log** na subseção **Configurações**.

   A janela **Inspeção do Log** é exibida.
5. Selecione a guia **Regras predefinidas**.
6. Marque ou desmarque a caixa de seleção **Aplicar regras predefinidas para inspeção do log**.

   Para que a tarefa seja executada, pelo menos uma regra de inspeção do log deve ser selecionada.
7. 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.
8. Para configurar as regras selecionadas, clique no botão **Configurações avançadas**.

A janela **Inspeção do Log** é exibida.

9. Na seção **Detecção de ataque de força bruta**, defina o número de tentativas e um período que serão considerados como acionadores para o analisador heurístico.

10. Na seção **Detecção de login de rede**, especifique o início e o fim do intervalo de tempo. O Kaspersky Embedded Systems Security for Windows considera as tentativas de login feitas durante esse intervalo como uma atividade anômala.

11. Selecione a guia **Exclusões**.

12. Execute as seguintes ações para adicionar usuários confiáveis:

    a. Clique no botão **Procurar**.

    b. Selecione um usuário.

    c. Clique no botão **OK**.

    O usuário selecionado é adicionado à lista de usuários confiáveis.

13. Execute as seguintes ações para adicionar endereços IP confiáveis:

    a. Insira o endereço IP.

    b. Clique no botão **Adicionar**.

14. O endereço IP inserido é adicionado à lista de endereços IP confiáveis.

15. Na guia **Gerenciamento da tarefa** configure a programação de inicialização da tarefa.

16. Clique no botão **OK** na janela **Inspeção do Log**.

A configuração da tarefa de Inspeção do Log é salva.

Adição das Regras de Inspeção do Log por meio do Plug-in de Administração

Execute as seguintes ações para adicionar e configurar uma nova regra de Inspeção do Log personalizada:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:

    - Para definir as configurações do aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

    - Para definir as configurações de uma tarefa ou aplicativo para um dispositivo protegido individual, selecione a guia **Dispositivos** e vá para configurações da tarefa local ou configurações do aplicativo.

4. Na seção **Inspeção do sistema**, clique no botão **Inspeção do Log** na subseção **Configurações**.

    A janela **Inspeção do Log** é exibida.

5. Na guia **Regras personalizadas**, marque ou desmarque a caixa de seleção **Aplicar regras personalizadas para inspeção do log**.

   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.

6. Para adicionar uma nova regra personalizada, clique no botão **Adicionar**.

   A janela **Regra personalizada de inspeção do log** é exibida.

7. Na seção **Geral**, especifique a seguinte informação sobre a nova regra:

   - **Nome da regra**
   - **A regra é acionada quando novas entradas aparecem no log de eventos do Windows se o identificador (ID) especificado for encontrado nos parâmetros do evento**

8. Na seção **Critérios para acionamento**, especifique os IDs de eventos que acionarão a regra:

   a. Insira um ID.

   b. Clique no botão **Adicionar**.

      O ID de evento inserido é adicionado à lista. É possível adicionar um número ilimitado de identificadores a cada regra.

9. Clique no botão **OK**.

   A regra de inspeção do log é adicionada à lista de regras.

Gerenciamento das regras de Inspeção do Log por meio do Console do Aplicativo

Nesta seção, saiba como adicionar e configurar regras de Inspeção do Log por meio do Console do Aplicativo.

Configuração de regras de tarefa predefinidas

Realize as seguintes ações para configurar o analisador heurístico para a tarefa de Inspeção do Log:

1. Na árvore do Console do Aplicativo, expanda o node **Inspeção do sistema**.
2. Selecione o node secundário **Inspeção do Log**.
3. Clique no link **Inspeção do Log** no painel de resultados do node **Propriedades**.

   A janela **Configurações de tarefa** é aberta.

4. Selecione a guia **Regras predefinidas**.
5. Marque ou desmarque a caixa de seleção **Aplicar regras predefinidas para inspeção do log**.

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, vá até a guia **Estendido**.
8. Na seção **Detecção de ataque de força bruta**, defina o número de tentativas e um período que serão considerados como acionadores para o analisador heurístico.
9. Na seção **Login da rede**, especifique o início e o fim do intervalo de tempo. O Kaspersky Embedded Systems Security for Windows considera as tentativas de login feitas durante esse intervalo como uma atividade anômala.
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 no botão **OK**.
    O 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**.
    O endereço IP inserido é adicionado à lista de endereços IP confiáveis.
13. Selecione as guias **Agendamento** e **Avançado** para configurar a programação de inicialização da tarefa.
14. Clique em **OK** na janela **Configurações de tarefa**.
    A configuração da tarefa de Inspeção do Log é salva.

Adição das regras de Inspeção do Log por meio do Console do Aplicativo

Para adicionar e configurar uma nova regra de Inspeção do Log personalizada:

1. Na árvore do Console do Aplicativo, expanda o node **Inspeção do sistema**.
2. Selecione o node secundário **Inspeção do Log**.
3. No painel de resultados do node **Inspeção do Log**, clique no link **Regras de inspeção do Log**.
4. A janela **Regras de inspeção do Log** é exibida.
5. Desmarque ou marque a caixa de seleção **Aplicar regras personalizadas para inspeção do log. As regras configuradas não são aplicadas até que a caixa de seleção seja marcada**. A soma de verificação é exibida no log de tarefas.

   É possível controlar se as regras predefinidas serão aplicadas à tarefa de Inspeção do Log. Marque as caixas de seleção correspondentes às regras que deseja aplicar à Inspeção do Log.

6. Para criar uma nova regra personalizada:
   a. Digite o nome da nova regra.
   b. Clique no botão **Adicionar**.
      A regra criada é adicionada à lista de regra geral.
7. Para configurar qualquer regra:
   a. Selecione uma regra na lista.
      Na área direita da janela, a guia **Descrição** exibe as informações gerais sobre a regra.

      A descrição da nova regra está em branco.

   b. Selecione a guia **Configurações de regra**.
8. Na seção **Geral**, especifique a seguinte informação sobre a nova regra:
   - **Nome da regra**
   - **Nome do log**
   - **A regra é acionada quando novas entradas aparecem no log de eventos do Windows se o identificador (ID) especificado for encontrado nos parâmetros do evento**
9. Na seção **Identificadores de eventos**, especifique os IDs do evento que acionarão a regra:
   a. Insira um ID de evento.
   b. Clique no botão **Adicionar**.
      O ID de evento inserido é adicionado à lista. É possível adicionar um número ilimitado de identificadores a cada regra.
10. Clique no botão **Salvar**.

As regras de Inspeção do Log configuradas serão aplicadas.

Gerenciamento das regras de Inspeção do Log por meio do Plug-in da Web

Para adicionar e configurar regras de Inspeção do Log por meio do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Inspeção do sistema**.
5. Clique no botão **Configurações** na subseção **Inspeção do Log**.
6. Defina as configurações descritas na tabela a seguir.

Configurações da tarefa de Inspeção do Log

Configuração	Descrição
Aplicar regras personalizadas para inspeção do log	Você pode ativar, desativar, adicionar ou alterar as regras personalizadas. A configuração que está disponível na tabela tem a lista de regras personalizadas.
Aplicar regras predefinidas para inspeção do log	É possível ativar ou desativar o analisador heurístico, que detecta atividades anormais no dispositivo protegido. A configuração que está disponível na tabela tem a lista de regras personalizadas.
Detectar ataque de força bruta se uma senha incorreta for inserida com a frequência definida	É possível definir o número de tentativas e o período, que serão considerados como acionadores pelo analisador heurístico.
Detectar login de rede se logado dentro de um período definido	É possível indicar o início e o fim do intervalo de tempo durante o qual o Kaspersky Embedded Systems Security for Windows encara tentativas de conexão como atividades anormais.
Exclusões de usuários	É possível especificar usuários que não acionarão o analisador heurístico.
Endereços IP excluídos	É possível especificar endereços IP que não acionarão o analisador heurístico.
Gerenciamento da tarefa	É possível definir configurações para a inicialização programada da tarefa.

Verificação por Demanda

Esta seção fornece informações sobre as tarefas de Verificação por Demanda e instruções sobre a definição de configurações da tarefa de Verificação por Demanda e configurações de segurança no dispositivo protegido.

Sobre tarefas de Verificação por Demanda

O Kaspersky Embedded Systems Security for Windows verifica a área especificada quanto à existência de vírus e outras ameaças à segurança do computador. O Kaspersky Embedded Systems Security for Windows verifica arquivos, RAM e objetos de execução automática do dispositivo protegido.

O Kaspersky Embedded Systems Security for Windows oferece as seguintes tarefas de Verificação por Demanda:

- A tarefa Verificação na Inicialização do Sistema Operacional é executada sempre que o Kaspersky Embedded Systems Security for Windows é iniciado. O aplicativo verifica setores de inicialização e registros mestres de inicialização de discos rígidos, unidades removíveis, da memória do sistema e da memória do processo. Cada vez que o Kaspersky Embedded Systems Security for Windows executa a tarefa, ele cria uma cópia dos setores de inicialização não infectados. Se, ao iniciar a tarefa novamente, ele detectar uma ameaça nesses setores, eles serão substituídos pela cópia de backup.

  A tarefa Verificação na inicialização do sistema operacional é criada automaticamente após a instalação. Por padrão, o modo Apenas notificar é aplicado. Nesse caso, depois de implementar o Kaspersky Embedded Systems Security for Windows nos dispositivos, será possível ativar a tarefa Verificação na inicialização do sistema operacional caso nenhum problema com os serviços do sistema tenha sido descoberto durante a verificação. Caso o aplicativo detecte serviços críticos do sistema como objetos infectados ou provavelmente infectados, o modo apenas notificação dará tempo para descobrir o motivo e resolver o problema. Se o aplicativo aplicar o modo Executar ação recomendada, que chama o método Desinfetar. Remova, caso a ação de desinfecção falhe, a desinfecção ou a remoção dos arquivos do sistema pode resultar em problemas críticos para a inicialização do sistema operacional.

  > A tarefa Verificação na Inicialização do Sistema Operacional pode não ser executada caso um dispositivo protegido acorde após o modo de suspensão ou hibernação. A tarefa é executada apenas na reinicialização do dispositivo protegido ou inicialização após o desligamento completo.

- Por padrão, a tarefa de Verificação de Áreas Críticas é executada semanalmente de acordo com uma programação. O Kaspersky Embedded Systems Security for Windows verifica objetos em áreas críticas do sistema operacional: objetos de execução automática, setores de inicialização e registros mestres de inicialização de discos rígidos e unidades removíveis, a memória do sistema e a memória do processo. O aplicativo verifica arquivos em pastas do sistema; por exemplo, %windir%\system32. O Kaspersky Embedded Systems Security for Windows aplica as configurações de segurança correspondentes ao nível Recomendado. Você pode modificar as configurações da tarefa de Verificação de Áreas Críticas.

- A tarefa de Verificação da Quarentena é executada por padrão de acordo com uma programação após cada atualização do banco de dados. O escopo da tarefa de Verificação da Quarentena não podem ser modificadas.

- A tarefa de Controle de Integridade de Aplicativos é executada diariamente. Ela fornece a opção de verificar módulos do Kaspersky Embedded Systems Security for Windows quanto à presença de danos ou de modificações. A pasta de instalação do aplicativo é marcada. As estatísticas de execução da tarefa indicam o número de módulos verificados e corrompidos. Os valores das configurações de tarefa são definidos por padrão e não podem ser editados. As configurações da programação de inicialização da tarefa podem ser editadas.

Adicionalmente, é possível criar tarefas de Verificação por Demanda personalizadas, por exemplo, uma tarefa para verificar pastas compartilhadas no dispositivo protegido.

O Kaspersky Embedded Systems Security for Windows pode executar várias tarefas de Verificação por Demanda simultaneamente.

Sobre o escopo da verificação e configurações de segurança da tarefa

No Console do Aplicativo, o escopo da verificação da tarefa de Verificação por Demanda é exibido em uma árvore ou na lista dos recursos de arquivos do dispositivo protegido que o Kaspersky Embedded Systems Security for Windows pode controlar. Por padrão, os recursos de arquivos de rede do dispositivo protegido são exibidos em um modo de visualização em lista.

No Plug-in de Administração, apenas a exibição de lista está disponível.

Para exibir recursos de arquivos de rede no modo de visualização em árvore no Console do Aplicativo,

abra a lista suspensa no setor superior esquerdo da janela de **Configurações do escopo da verificação** e selecione **Visualização em árvore**.

Os itens ou nós são exibidos em um modo de visualização de lista ou em árvore dos recursos de arquivos do dispositivo protegido, como se segue:

☑ O nó está incluído no escopo de verificação.

☐ O nó é excluído do escopo de verificação.

☑ Pelo menos um dos nodes secundários deste nó é excluído do escopo de verificação ou as configurações de segurança do(s) nó(s) filho(s) são diferentes da configuração de um node principal (somente para um modo de visualização em árvore).

O ícone ☑ é exibido se todos os nodes secundários forem selecionados, mas se o node principal não for selecionado. Neste caso, as modificações na composição dos arquivos e das pastas do node principal são desconsideradas automaticamente quando o escopo da verificação do node secundário selecionado estiver sendo criado.

Usando o Console do Aplicativo, também é possível adicionar unidades virtuais ao escopo da verificação. Os nomes dos nodes virtuais são exibidos em azul.

Configurações de segurança

Na tarefa de Verificação por Demanda selecionada, as configurações de segurança padrão podem ser modificadas ao defini-las como configurações comuns para todo o escopo da proteção ou da verificação, ou como configurações diferentes para nós ou itens diferentes na árvore ou lista de recursos de arquivos do dispositivo.

As configurações de segurança definidas para o node principal selecionado são automaticamente aplicadas a todos os nodes secundários. As configurações de segurança do node principal não são aplicadas a nós filhos configurados separadamente.

As configurações de um escopo de verificação ou escopo da proteção selecionado podem ser definidas usando um dos seguintes métodos:

- Selecione um de três níveis de segurança predefinidos (**Desempenho máximo**, **Recomendado** ou **Proteção máxima**).

- Modifique manualmente as configurações de segurança para os nodes ou itens selecionados na árvore ou lista dos recursos de arquivos do dispositivo protegido (o nível de segurança é alterado para **Personalizado**).

O conjunto de configurações de um nó pode ser salvo em um modelo para ser aplicado posteriormente a outros nodes.

Escopos de verificação predefinidos

A árvore ou a lista de recursos de arquivo do dispositivo protegido para a tarefa de Verificação por Demanda selecionada é exibida na janela **Configurações do escopo da verificação**.

A árvore ou lista de recursos de arquivos exibe os nodes aos quais você tem acesso à leitura com base nas configurações de segurança definidas no Microsoft Windows.

O Kaspersky Embedded Systems Security for Windows contém os escopos de verificação predefinidos a seguir:

- **Meu Computador**. O Kaspersky Embedded Systems Security for Windows verifica o dispositivo protegido inteiro.
- **Discos rígidos locais**. O Kaspersky Embedded Systems Security for Windows verifica objetos nos discos rígidos de um dispositivo protegido. É possível incluir ou excluir do escopo da verificação todos os discos rígidos, discos, pastas ou arquivos individuais.
- **Unidades removíveis**. O Kaspersky Embedded Systems Security for Windows verifica arquivos em dispositivos externos, como CDs ou drives removíveis. É possível incluir ou excluir do escopo da verificação todas as unidades removíveis, discos individuais, pastas ou arquivos individuais.
- **Rede**. Pastas ou arquivos de rede podem ser adicionados ao escopo da verificação especificando seu caminho no formato UNC (Universal Naming Convention). A conta usada para iniciar a tarefa deve ter permissões de acesso às pastas e aos arquivos de rede adicionados. Por padrão, as tarefas de Verificação por Demanda são executadas com a conta do sistema.

  As unidades de rede conectadas também não serão exibidas na árvore de recursos de arquivos do dispositivo protegido. Para incluir objetos das unidades de rede no escopo da verificação, especifique o caminho da pasta que corresponde à unidade de rede no formato UNC.

- **Memória do sistema**. O Kaspersky Embedded Systems Security for Windows verifica os arquivos executáveis e módulos dos processos em execução no sistema operacional quando a verificação é iniciada.
- **Objetos de inicialização**. O Kaspersky Embedded Systems Security for Windows verifica objetos referidos por chaves do registro e arquivos de configuração, por exemplo, WIN.INI ou SYSTEM.INI, bem como os módulos do aplicativo iniciados automaticamente na inicialização do dispositivo protegido.
- **Pastas compartilhadas**. Você pode incluir pastas compartilhadas no dispositivo protegido no escopo da verificação.
- **Unidades virtuais**. Pastas, arquivos e unidades virtuais conectadas ao dispositivo protegido podem ser incluídas no escopo da verificação; por exemplo, unidades de cluster comuns.

As unidades virtuais criadas usando um comando SUBST não são exibidas na árvore de recursos de arquivos do dispositivo protegido no Console do Aplicativo. Para verificar objetos em uma unidade virtual, inclua a pasta do dispositivo protegido associada a essa unidade virtual no escopo da verificação.

Os escopos de verificação padrão são exibidos na árvore de recursos de arquivos de rede por padrão. Eles podem ser adicionados na lista de recursos de arquivos de rede quando ela é criada nas configurações do escopo da verificação.

Por padrão, as tarefas de Verificação por Demanda são executadas nos seguintes escopos:

- Tarefa de Verificação na Inicialização do Sistema operacional:
  - **Discos rígidos locais**.
  - **Unidades removíveis**.
  - **Memória do sistema**.
- Verificação de áreas críticas:
  - **Discos rígidos locais** (excluindo pastas Windows)
  - **Unidades removíveis**.
  - **Memória do sistema**.
  - **Objetos de inicialização**.
- Outras tarefas:
  - **Discos rígidos locais** (excluindo pastas Windows)
  - **Unidades removíveis**.
  - **Memória do sistema**.
  - **Objetos de inicialização**.
  - **Pastas compartilhadas**.

Verificação de arquivos no armazenamento on-line

Sobre arquivos na nuvem

O Kaspersky Embedded Systems Security for Windows pode interagir com arquivos na nuvem do Microsoft OneDrive. O aplicativo é compatível com o novo recurso de arquivos sob demanda do OneDrive.

O Kaspersky Embedded Systems Security for Windows não é compatível com outros armazenamentos on-line.

O recurso Arquivos por Demanda do OneDrive ajuda você a acessar todos os seus arquivos do OneDrive sem precisar baixar todos eles e usar o espaço de armazenamento do seu dispositivo. Você pode baixar arquivos no seu disco rígido quando precisar.

Quando o recurso de Arquivos por 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. Não é possível 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 no disco rígido e sempre está disponível*.

Verificação de arquivo na nuvem

O Kaspersky Embedded Systems Security for Windows só pode verificar arquivos na nuvem armazenados localmente em um dispositivo protegido. Esses arquivos do OneDrive têm o status e . Os arquivos são ignorados durante a verificação, já que não estão fisicamente localizados no dispositivo protegido.

> O Kaspersky Embedded Systems Security for Windows não baixa automaticamente arquivos da nuvem durante a verificação, mesmo se eles estiverem incluídos no escopo da verificação.

Os arquivos na nuvem são processados por várias tarefas do Kaspersky Embedded Systems Security for Windows em vários cenários, dependendo do tipo de tarefa:

- Verificação de arquivo na nuvem em tempo real: é possível adicionar pastas que contenham arquivos da nuvem ao escopo da proteção da tarefa de Proteção de Arquivos em Tempo Real. Arquivos são verificados quando são acessados 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 na 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 na nuvem, e que não existe em uma unidade local.

- Geração e uso de regras de controle de inicialização de aplicativos: é possível criar regras de permissão e negação para arquivos e usando a tarefa 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 na nuvem.

  > A tarefa de Controle de Inicialização de Aplicativos bloqueia o início de todos os arquivos na nuvem, independentemente do status. Os arquivos não estão incluídos no escopo da geração de regras do aplicativo, já que não estão fisicamente armazenados no disco rígido. Já que regras de permissão não podem ser criadas para tais arquivos, eles ficam sujeitos ao princípio de Negação padrão.

Quando uma ameaça for detectada em um arquivo na 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.

Sobre níveis de segurança predefinidos

As configurações de segurança **Usar a tecnologia iChecker**, **Usar a tecnologia iSwift**, **Usar o analisador heurístico** e **Verificar assinatura da Microsoft nos arquivos** não são incluídas nas configurações para os níveis de segurança predefinidos. Se as configurações **Usar a tecnologia iChecker**, **Usar a tecnologia iSwift**, **Usar o analisador heurístico** e **Verificar assinatura da Microsoft nos arquivos** forem alteradas, o nível de segurança predefinido selecionado não será alterado.

É possível aplicar um dos quatro seguintes níveis de segurança predefinidos para um nó selecionado na árvore de recursos de arquivos do dispositivo: **Desempenho máximo**, **Recomendado**, **Proteção máxima** ou **Somente notificações**. Cada um dos níveis contém suas próprias configurações de segurança predefinidas (veja a tabela abaixo).

Desempenho máximo

O nível de segurança **Desempenho máximo** é recomendado se a rede tiver medidas de segurança adicionais nos dispositivos protegidos, como firewalls e políticas de segurança existentes, além de usar o Kaspersky Embedded Systems Security for Windows nos dispositivos protegidos.

Recomendado

O nível de segurança **Recomendado** assegura a melhor combinação de impacto de proteção e desempenho nos dispositivos. Os especialistas da Kaspersky recomendam esse nível como adequado para proteger dispositivos 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 de dispositivos.

Somente notificações

O nível de segurança **Somente notificações** é recomendado caso haja muitos computadores potencialmente infectados na rede corporativa, e bloqueá-los poderia interromper significativamente a operação da organização.

Níveis de segurança predefinidos e valores de configurações de segurança correspondentes

Opções	Nível de segurança			
	Desempenho	Recomendado	Proteção máxima	Somente

	máximo			notificações
Verificar objetos	Por formato	Todos os objetos	Todos os objetos	Todos os objetos
Verificar apenas arquivos novos e modificados	Ativado	Desativado	Desativado	Desativado
Ação a ser executada em objetos infectados e outros	Desinfectar. Remover, caso a desinfecção falhe	Executar a ação recomendada pelos especialistas da Kaspersky	Desinfectar. Remover, caso a desinfecção falhe	Somente notificações
Ação a ser executada em objetos possivelmente infectados	Quarentena	Executar a ação recomendada pelos especialistas da Kaspersky	Quarentena	Somente notificações

Os objetos críticos do sistema são arquivos necessários para a operação do sistema operacional e do Kaspersky Embedded Systems Security for Windows. Esses arquivos não podem ser excluídos. Os processos associados a esses objetos não podem ser encerrados.

Excluir arquivos	Não	Não	Não	Não
Não detectar	Não	Não	Não	Não
Parar a verificação se demorar mais que (s)	60 s	Não	Não	Não
Não verificar objetos compostos com mais de (MB)	8 MB	Não	Não	Não
Verificar fluxos NTFS alternativos	Sim	Sim	Sim	Sim
Verificar setores de inicialização do disco e MBR	Sim	Sim	Sim	Sim
Verificação de objetos compostos	• Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* * Somente objetos novos e modificados	• Arquivos compactados* • Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* * Todos os objetos	• Arquivos compactados* • Arquivos compactados SFX* • Bancos de dados de e-mail* • E-mails sem formatação* • Objetos compactados*	• Arquivos compactados* • Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* * Todos os objetos

			• Objetos OLE incorporados* * Todos os objetos	

Verificação de unidades removíveis

É possível configurar a verificação de unidades removíveis conectadas ao dispositivo protegido por meio da porta USB.

O Kaspersky Embedded Systems Security for Windows 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 unidades removíveis. Não é possível definir as configurações da tarefa temporária de Verificação por Demanda.

Se você instalou o Kaspersky Embedded Systems Security for Windows sem os bancos de dados de antivírus, a verificação de unidades removíveis ficará indisponível.

O Kaspersky Embedded Systems Security for Windows verifica os drives removíveis conectados quando são registrados como dispositivos externos 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 for Windows permite o acesso a unidades removíveis durante a verificação.

Os resultados da verificação para cada unidade removível estão disponíveis no log de tarefas para a Verificação por Demanda criada quando a unidade removível for conectada.

É possível alterar as configurações do componente de Verificação de unidades removíveis (consulte a tabela abaixo).

Configurações de verificação de unidades removíveis

Configuração	Valor padrão	Descrição
Verificar unidades removíveis ao conectar via USB	Desmarcada	É possível ligar e desligar a verificação de unidades removíveis após a conexão via USB com o dispositivo protegido.
Verificar unidades removíveis se o volume de dados armazenados não exceder (MB)	8192 MB	É possível reduzir o escopo do componente configurando o volume máximo de dados na unidade verificada. O Kaspersky Embedded Systems Security for Windows não verifica uma unidade removível se o volume de dados armazenados exceder o valor especificado.
Verificação com nível de segurança	Proteção máxima	É possível configurar 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.

Sobre a tarefa do Monitor de Comparação de Integridade de Arquivos

Durante a tarefa do Monitor de Comparação de Integridade de Arquivos, o Kaspersky Embedded Systems Security for Windows não verifica arquivos bloqueados, pastas, atalhos de arquivos e arquivos na nuvem.

A tarefa de Monitor de Comparação de Integridade de Arquivos monitora a integridade dos arquivos no escopo de monitoramento comparando o hash dos arquivos (MD5 ou SHA256) com uma linha de base.

Na primeira execução da tarefa de Monitor de Comparação de Integridade de Arquivos, o Kaspersky Embedded Systems Security for Windows cria uma linha de base calculando e armazenando o hash dos arquivos no escopo de monitoramento da tarefa. Se um escopo de monitoramento de tarefa do Monitor de Comparação de Integridade de Arquivos for alterado, o Kaspersky Embedded Systems Security for Windows atualizará a linha de base na próxima tarefa do monitor de comparação de integridade de arquivos executada calculando e armazenando o hash dos arquivos no escopo de monitoramento da tarefa. Se uma tarefa do Monitor de Comparação de Integridade de Arquivos foi excluída, o Kaspersky Embedded Systems Security for Windows exclui a linha de base desta tarefa do monitor de integridade do arquivo de linha de base.

Você pode excluir uma linha de base sem excluir a tarefa de Monitor de Comparação de Integridade de Arquivos usando a linha de comando.

A tarefa de Monitor de Comparação de Integridade de Arquivos rastreia as seguintes alterações de arquivos no escopo de monitoramento:

- o escopo de monitoramento contém um arquivo que não está presente na linha de base
- o escopo de monitoramento não contém um arquivo presente na linha de base
- o hash de um arquivo no escopo de monitoramento difere do hash desse arquivo em uma linha de base

A tarefa de Monitor de Comparação de Integridade de Arquivos não rastreia alterações nos atributos e fluxos alternativos do arquivo.

Se um arquivo ou uma pasta estiver inacessível, o Kaspersky Embedded Systems Security for Windows não o adicionará à linha de base durante sua criação e criará um evento de falha no cálculo da soma de verificação do arquivo durante a execução da tarefa de Monitor de Comparação de Integridade de Arquivos.

Um arquivo ou uma pasta pode estar inacessível pelos seguintes motivos:

- o caminho especificado não existe
- um tipo de arquivo especificado pela máscara não está presente no caminho especificado
- o arquivo especificado está bloqueado

- o arquivo especificado está vazio

Ativação do início da tarefa de Verificação por Demanda no menu de contexto

Você pode ativar o início da tarefa de Verificação por Demanda para um ou vários arquivos em um menu de contexto no Microsoft Windows Explorer.

Para ativar o início da tarefa de Verificação por Demanda em um menu de contexto:

1. Crie os seguintes arquivos REG:

```
Editor do Registro do Windows versão 5.0.0

[HKEY_CLASSES_ROOT\Directory\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\*\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\Directory\shell\kess]

@="Scan with Kaspersky Embedded Systems Security for Windows\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\Directory\shell\kess\DefaultIcon]

@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess]

@="Scan with Kaspersky Embedded Systems Security for Windows\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers]

"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavshell.exe"="~ RUNASADMIN"
```

> Você precisa especificar o local real da pasta de instalação do Kaspersky Embedded Systems Security.

2. Crie o arquivo `scan.cmd` com o seguinte conteúdo:

```
@echo off
set LOGNAME=%RANDOM%

"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems
Security\kavshell.exe" scan "%~1" /W:c:\temp\%LOGNAME%.txt

A verificação echo está em andamento...
type c:\temp\%LOGNAME%.txt
del c:\temp\%LOGNAME%.txt
```

```
timeout /t -1
```

O arquivo `scan.cmd` deve conter as seguintes informações:

- A localização do arquivo `kavshell.exe`.
- A localização do arquivo temporário que contém os resultados da verificação.
- Os parâmetros do comando `KAVSHELL SCAN`.
- O valor do tempo limite para fechar a janela do console quando a tarefa for concluída.

3. Copie o arquivo `scan.cmd` na pasta especificada do arquivo REG `[HKEY_CLASSES_ROOT\Directory\shell\kess\command]`.

   No exemplo, a pasta `C:\Temp` é utilizada.

Não é necessário reiniciar o sistema operacional.

Configurações padrão das tarefas de Verificação por Demanda

Por padrão, as tarefas de Verificação por Demanda possuem as configurações descritas na tabela abaixo. É possível configurar tarefas locais do sistema de Verificação por Demanda e tarefas personalizadas.

Configurações padrão das tarefas de Verificação por Demanda

Configuração	Valor padrão	Descrição
Escopo da verificação	Aplicado em tarefas locais do sistema e tarefas personalizadas: • **Verificação na Inicialização do Sistema Operacional**: o dispositivo protegido inteiro, excluindo pastas compartilhadas e objetos de execução automática. • **Verificação de Áreas Críticas**: o dispositivo protegido inteiro, excluindo pastas compartilhadas e certos	Você pode alterar o escopo da verificação. O escopo da verificação não pode ser configurado para as tarefas locais do sistema de **Verificação da Quarentena** e **Controle de Integridade de Aplicativos**. A tarefa **Verificação na Inicialização do Sistema Operacional** é criada automaticamente após a instalação. Por padrão, o modo **Apenas notificar** é aplicado. Nesse caso, depois de implementar o Kaspersky Embedded Systems Security for Windows nos dispositivos, será possível ativar a tarefa **Verificação na Inicialização do Sistema Operacional** caso nenhum problema com os serviços do sistema tenha sido descoberto durante a verificação. Caso o aplicativo detecte serviços críticos do sistema como objetos infectados ou provavelmente infectados, o modo **Apenas notificação** dará tempo para descobrir o motivo e resolver o problema. Se o aplicativo aplicar o modo **Executar ação recomendada**, que chama o método **Desinfetar.** Ação **Remover se a desinfecção falhar**. A desinfecção ou remoção dos arquivos do sistema pode resultar em problemas críticos com a inicialização do sistema operacional.

	arquivos de sistema operacional. • **Verificação por demanda** (tarefas personalizadas): o dispositivo protegido inteiro.	
Configurações de segurança	As configurações comuns de todo o escopo da verificação correspondem ao nível de segurança **Recomendado**.	Para os nodes selecionados na lista ou na árvore de recursos de arquivos do dispositivo protegido, é possível: • Selecionar um nível de segurança predefinido diferente • Alterar manualmente as configurações de segurança É possível salvar um grupo de configurações de segurança para um nó selecionado como um modelo para ser usado posteriormente para outro node.
Usar o analisador heurístico	É usado com o nível de análise **Médio** para Verificação de Áreas Críticas, Verificação na Inicialização do Sistema Operacional e tarefas personalizadas. É usado com o nível de análise **Profundo** para a tarefa de Verificação da Quarentena.	É possível ativar ou desativar o Analisador Heurístico e configurar o nível de análise. O nível de análise da tarefa de Verificação da quarentena não pode ser configurado. O analisador heurístico não é usado na tarefa de Controle de Integridade de Aplicativos e tarefas do Monitor de Comparação de Integridade de Arquivos.
Aplicar Zona Confiável	Aplicado (Não aplicado a tarefa de Verificação da Quarentena)	Lista geral de exclusões que podem ser usadas em tarefas selecionadas.
Usar a KSN para verificação	Aplicada.	É possível melhorar a proteção do dispositivo usando a infraestrutura do serviço na nuvem da Kaspersky Security Network.
Configurações para iniciar uma tarefa com permissões específicas	A tarefa é iniciada em uma conta do sistema.	É possível editar configurações de inicialização de tarefas com permissões de conta específicas para todas as tarefas de Verificação por Demanda do sistema e personalizadas, exceto tarefas de Verificação da Quarentena e de Controle de Integridade de Aplicativos.
Executar tarefa em	Não aplicado	Você pode configurar o nível de prioridade das tarefas de Verificação por Demanda.

segundo plano (baixa prioridade)		
Programação de inicialização da tarefa	Aplicado em tarefas locais do sistema: • Verificação na Inicialização do Sistema operacional - **Ao iniciar o aplicativo** • Verificação de Áreas Críticas - **Semanalmente** • Verificação da Quarentena - **Após a atualização do banco de dados do aplicativo** • Controle de Integridade de Aplicativos - **Diariamente** Não usado em tarefas personalizadas criadas recentemente.	É possível definir as configurações para o início de uma tarefa programada.
Registro de execução da verificação e da atualização do status de proteção do dispositivo	O status de proteção do dispositivo é atualizado semanalmente após a Verificação de áreas críticas ser executada.	Você pode definir configurações para registrar a execução da Verificação de áreas críticas das seguintes maneiras: • Editar as configurações da programação de inicialização da tarefa de Verificação de áreas críticas. • Editar o escopo da verificação da tarefa de Verificação de áreas críticas. • Criar uma tarefa de Verificação por Demanda personalizada.

Gerenciando tarefas de Verificação por Demanda por meio do Plugin de Administração

Nesta seção, saiba como navegar pela interface do Plug-in de Administração e definir configurações de tarefa para um ou todos os dispositivos protegidos na rede.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura do assistente da tarefa de Verificação por Demanda

Para começar a criar uma nova tarefa de Verificação por Demanda personalizada:

1. Para criar uma tarefa local:

   a. Expanda o node **Dispositivos gerenciados** no Console de Administração do Kaspersky Security Center.

   b. Selecione o grupo de administração ao qual o dispositivo protegido pertence.

   c. No painel de resultados, na guia **Dispositivos**, abra o menu de contexto do dispositivo protegido.

   d. Selecione a opção de menu **Propriedades**.

   e. Na janela exibida, clique no botão **Adicionar** na seção **Tarefas**.

   A janela **Assistente de Nova Tarefa** será aberta.

2. Para criar uma tarefa de grupo:

   a. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

   b. Selecione o grupo de administração para o qual você deseja criar uma tarefa.

   c. Abra a guia **Tarefas**.

   d. Clique no botão **Nova tarefa**.

   A janela **Assistente de Nova Tarefa** será aberta.

3. Para criar uma tarefa para um grupo personalizado do dispositivo protegido:

   a. No node **Seleções de dispositivos** na árvore do Console de Administração do Kaspersky Security Center, clique no botão **Executar seleção** para executar uma seleção de dispositivo.

   b. Abra a guia **Resultados da seleção "nome da seleção"**.

   c. Na lista suspensa **Executar seleção**, selecione a opção **Criar uma tarefa para um resultado de seleção**.

   A janela **Assistente de Nova Tarefa** será aberta.

4. Selecione a tarefa **Verificação por demanda** na lista de tarefas disponíveis para o Kaspersky Embedded Systems Security for Windows.

5. Clique no botão **Avançar**.

A janela **Configurações** é exibida.

Defina as configurações da tarefa conforme necessário.

Para configurar uma tarefa de Verificação por Demanda existente,

Clique duas vezes no nome da tarefa na lista de tarefas no Kaspersky Security Center.

A janela **Propriedades: Verificação por demanda** é exibida.

Abertura das propriedades da tarefa de Verificação por Demanda

Para abrir as propriedades do aplicativo para a tarefa de Verificação por Demanda para um único dispositivo protegido:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração ao qual o dispositivo protegido pertence.
3. Selecione a guia **Dispositivos**.
4. Clique duas vezes no nome do dispositivo protegido para o qual deseja configurar o escopo da verificação.
   A janela **Propriedades: <Nome do dispositivo protegido>** é exibida.
5. Selecione a seção **Tarefas**.
6. Na lista de tarefas criadas para o dispositivo, selecione a tarefa de Verificação por Demanda que você criou.
7. Clique no botão **Propriedades**.
   A janela **Propriedades: Verificação por demanda** é exibida.

Defina as configurações da tarefa conforme necessário.

Criando uma tarefa de Verificação por Demanda

Para começar a criar uma nova tarefa de Verificação por Demanda personalizada:

1. Abra a janela **Configurações** no Assistente para Novas Tarefas.
2. Selecione o **Método de criação da tarefa** necessário.
3. Clique no botão **Avançar**.
4. Crie um escopo de verificação na janela **Escopo da verificação**:

Por padrão, o escopo da verificação inclui áreas críticas do dispositivo protegido. Os escopos de verificação são marcados na tabela com o ícone ☑. Os escopos de 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, pasta, objeto de rede ou arquivo no dispositivo protegido ou em outro dispositivo protegido na 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** na janela **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.
- Para ignorar objetos incorporados no escopo da verificação adicionado:
  a. Abra o menu de contexto na tabela **Escopo da verificação** e selecione **Adicionar exclusão**.
  b. Especifique os objetos a serem excluídos: selecione o escopo predefinido na lista **Escopo predefinido**, especifique o disco, a pasta, o objeto de rede ou o arquivo no dispositivo protegido ou em outro dispositivo protegido na rede.
  c. Clique no botão **OK**.

5. Na janela **Opções**, configure o analisador heurístico e a integração com outros componentes:
   - Configurar o uso do Analisador Heurístico.
   - Selecione a caixa **Aplicar Zona Confiável** se desejar excluir os objetos adicionados à lista da Zona Confiável do escopo da verificação da tarefa.

- Marque a caixa de seleção **Usar a KSN para verificação** se quiser usar os serviços na nuvem da Kaspersky Security Network para a tarefa.
- Para atribuir a prioridade *Baixa* ao processo de trabalho onde a tarefa será executada, marque 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 for Windows são executadas têm prioridade *Média* (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**.

6. Clique no botão **Avançar**.
7. Na janela **Agendamento**, especifique as configurações da programação de inicialização da tarefa.
8. Clique no botão **Avançar**.
9. Na janela **Seleção de uma conta para a execução da tarefa**, especifique a conta que deseja usar.
10. Clique no botão **Avançar**.
11. Especifique um nome de tarefa.
12. Clique no botão **Avançar**.

    O nome da tarefa não deve ter mais de 100 caracteres e não pode conter os seguintes símbolos: " * < > & \ : |

    A janela **Concluir a criação da tarefa** é exibida.

13. Você também pode executar a tarefa após a finalização do Assistente marcando a caixa de seleção **Executar a tarefa após a finalização do Assistente**.
14. Clique em **Concluir** para concluir a criação da tarefa.

A nova tarefa de Verificação por Demanda será criada para o dispositivo protegido selecionado ou um grupo de dispositivos protegidos.

Atribuindo o status de Verificação de Áreas Críticas a uma tarefa de Verificação por Demanda

Por padrão, o Kaspersky Security Center atribui o status *Aviso* ao dispositivo protegido se a tarefa Verificação de Áreas Críticas for executada com menos frequência do que especificado pelo limite de geração de eventos *A Verificação de áreas críticas não é realizada há muito tempo* no Kaspersky Embedded Systems Security for Windows.

Para configurar a verificação de todos os dispositivos protegidos 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 dispositivos protegidos no 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 dispositivos protegidos ou, mais tarde, na janela **Propriedades: <Nome da tarefa>**.

3. Ao utilizar uma política nova ou existente, desative o início programado de tarefas locais de Verificação por Demanda do sistema nos dispositivos protegidos do grupo.

O servidor de administração do Kaspersky Security Center avaliará então o status de segurança do dispositivo protegido. O servidor enviará uma notificação sobre o status de acordo com os resultados da última execução de uma tarefa com o status de Verificação de áreas críticas em vez de fazer isso tendo como referência os resultados da tarefa local do sistema de Verificação de áreas críticas.

É possível atribuir o status *Verificação de Áreas Críticas* às tarefas de grupo de Verificação por Demanda e a tarefas de grupos de dispositivos protegidos.

O Console do Aplicativo pode ser usado para visualizar se uma 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.

Execução de uma tarefa de Verificação por Demanda em segundo plano

Por padrão, é atribuída a prioridade *Médio(Normal)* aos processos nos quais as tarefas do Kaspersky Embedded Systems Security for Windows são executadas.

Um processo que executará a tarefa de Verificação por Demanda pode receber uma prioridade *Baixa*. Ao reduzir a prioridade do processo, o tempo necessário para executar a tarefa aumenta, mas isso pode ter um efeito positivo no desempenho dos processos de outros programas em execução.

É possível executar várias tarefas em segundo plano em um único processo de trabalho com prioridade baixa. É possível especificar o número máximo de processos para tarefas de Verificação por Demanda em segundo plano.

Para alterar a prioridade de uma tarefa de Verificação por Demanda existente:

1. Abra a janela **Propriedades: Verificação por demanda**.
2. Selecione ou desmarque a caixa **Executar tarefa em segundo plano**.
3. Clique no botão **OK**.

As configurações de tarefa definidas serão salvadas e aplicadas imediatamente à uma tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

Registrando a execução de uma Verificação de Áreas Críticas

Por padrão, o status de proteção do dispositivo é exibido no painel de resultados do node do **Kaspersky Embedded Systems Security for Windows** e atualizado semanalmente após a execução da tarefa de Verificação de Áreas Críticas.

A hora da atualização de status de proteção do dispositivo está vinculada com a programação da tarefa de Verificação por Demanda para a qual a caixa de seleção **Considerar tarefa como verificação de áreas críticas** está marcada. Por padrão, a caixa é selecionada somente para a tarefa de Verificação de áreas críticas e não pode ser modificada para esta tarefa.

Você pode selecionar a tarefa de Verificação por Demanda vinculada ao status de proteção do dispositivo apenas no Kaspersky Security Center.

Configuração do escopo da verificação da tarefa

Caso modifique o escopo da verificação nas tarefas de Verificação na inicialização do sistema operacional e Verificação de áreas críticas, será possível restaurar o escopo padrão da verificação nessas tarefas reparando o próprio Kaspersky Embedded Systems Security for Windows (**Iniciar** > **Programas** > **Kaspersky Embedded Systems Security for Windows** > **Modificar ou remover o Kaspersky Embedded Systems Security for Windows**). No assistente de instalação, selecione **Reparar componentes instalados** e clique em **Avançar**. Em seguida, marque a caixa de seleção **Restaurar configurações recomendadas do aplicativo**.

Para configurar o escopo da verificação de uma tarefa de Verificação por Demanda existente:

1. Abra a janela **Propriedades: Verificação por demanda**.
2. Selecione a guia **Escopo da verificação**.
3. Para incluir itens no escopo da verificação:
   a. Abra o menu de contexto em uma parte vazia da lista do escopo da verificação.
   b. Selecione a opção **Adicionar escopo** ono menu de contexto.
   c. Na janela aberta **Adicionar objetos ao escopo da verificação**, selecione um tipo de objeto que deseja adicionar:
      - **Escopo predefinido** – para adicionar um dos escopos predefinidos em um dispositivo protegido. Em seguida, na lista suspensa, selecione o escopo da verificação desejado.
      - **Disco, pasta ou local de rede** – para incluir uma unidade individual, pasta ou objeto de rede no escopo da verificação. Em seguida, selecione o escopo desejado clicando no botão **Procurar**.
      - **Arquivo** – para incluir um arquivo individual no escopo da verificação. Em seguida, selecione o escopo desejado clicando no botão **Procurar**.

   Não é possível adicionar um objeto a um escopo da verificação se ele já tiver sido adicionado como uma exclusão do escopo da verificação.
4. Para excluir nós individuais do escopo da verificação, desmarque as caixas ao lado dos nomes destes nós ou siga as etapas a seguir:

a. Abra o menu de contexto no escopo da verificação clicando com o botão direito nele.

b. No menu de contexto, selecione a opção **Adicionar exclusão**.

c. Na janela **Adicionar exclusão**, selecione um tipo de objeto que deseja adicionar como uma exclusão do escopo da verificação seguindo o procedimento usado ao adicionar um objeto ao escopo da verificação.

5. Para modificar o escopo da verificação ou uma exclusão adicionada, selecione a opção **Editar escopo** no menu de contexto do escopo da verificação correspondente.

6. Para ocultar um escopo da verificação ou exclusão adicionados anteriormente na lista de recursos de arquivos de rede, selecione a opção **Remover escopo** no menu de contexto do escopo de verificação necessário.

   O escopo da verificação é excluído do escopo da tarefa de Verificação por Demanda quando ele é removido da lista de recursos de arquivos de rede.

7. Clique no botão **OK**.

A janela Configurações do escopo da verificação é fechada. As configurações recém-definidas são salvas.

Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda

É possível aplicar um dos seguintes três níveis de segurança predefinidos para um nó selecionado na lista de recursos de arquivos do dispositivo protegido: **Desempenho máximo**, **Recomendado** e **Proteção máxima**.

Para selecionar um dos níveis de segurança predefinidos:

1. Abra a janela Propriedades: Verificação por demanda.

2. Selecione a guia **Escopo da verificação**.

3. Na lista do dispositivo protegido, selecione um item incluído no escopo da verificação para definir um nível de segurança predefinido.

4. Clique no botão **Configurar**.

   A janela **Configurações da verificação por demanda** é exibida.

5. Na guia **Nível de segurança**, selecione o nível de segurança a ser aplicado.

   A janela exibe a lista de configurações de segurança correspondentes ao nível de segurança selecionado.

6. Clique no botão **OK**.

7. Clique no botão **OK** na janela **Propriedades: Verificação por demanda**.

   As configurações de tarefa definidas serão salvadas e aplicadas imediatamente à uma tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

Definição manual de configurações de segurança

Por padrão, as tarefas de Verificação por Demanda usam configurações de segurança comuns para o escopo da verificação inteiro.

Estas configurações correspondem ao nível de segurança predefinido **Recomendado**.

Os valores padrão das configurações de segurança podem ser modificados, definindo-os como configurações comuns para todo o escopo da verificação ou como configurações diferentes para itens diferentes na lista de recursos de arquivos ou nós da árvore do dispositivo protegido.

Para definir as configurações de segurança manualmente:

1. Abra a janela **Propriedades: Verificação por demanda**.
2. Selecione a guia **Escopo da verificação**.
3. Selecione os itens na lista do escopo da verificação cujas configurações de segurança você deseja definir.

   Um modelo predefinido de configurações de segurança pode ser aplicado em um nó ou item selecionado no escopo da verificação.

4. Clique no botão **Configurar**.

   A janela **Configurações da verificação por demanda** é exibida.

5. Defina as configurações de segurança para o node ou item selecionado de acordo com seus requisitos:

   - **Geral**
   - **Ações**
   - **Desempenho**
   - **Armazenamento hierárquico**

6. Clique no botão **OK** na janela **Configurações da verificação por demanda**.
7. Clique no botão **OK** na janela **Escopo da verificação**.

As novas configurações de escopo da verificação são salvas.

Definir configurações gerais de tarefas

Para definir as configurações gerais da tarefa de Verificação por Demanda:

1. Abra a janela **Propriedades: Verificação por demanda**.
2. Selecione a guia **Escopo da verificação**.
3. Clique no botão **Configurar**.

   A janela **Configurações da verificação por demanda** é exibida.

4. Clique no botão **Configurações**.

5. Na guia **Geral** do grupo **Verificar objetos**, especifique os tipos de objetos que deseja incluir no escopo da verificação:

   - **Objetos a serem verificados**:
     - Todos os objetos
     - Objetos verificados por formato
     - Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus
     - Objetos verificados pela lista de extensões especificada
   - **Subpastas**
   - **Subarquivos**
   - Verificar setores de inicialização do disco e MBR
   - Verificar fluxos NTFS alternativos

6. No grupo **Desempenho**, selecione ou desmarque a caixa Verificar apenas arquivos novos e modificados.

   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.

7. No grupo **Verificação de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da verificação:

   - Todos/Apenas novos arquivos compactados
   - Todos/Apenas novos arquivos compactados SFX
   - Todos/Apenas novos bancos de dados de e-mail
   - Todos/Apenas novos objetos compactados
   - Todos/Apenas novos e-mails sem formatação
   - Todos/Apenas novos objetos OLE incorporados

8. Clique no botão **OK**.

A nova configuração de tarefa será salva.

Configurar ações

Para configurar ações em objetos infectados e outros objetos detectados durante a tarefa de Verificação por Demanda:

1. Abra a janela Propriedades: Verificação por demanda.

2. Selecione a guia **Escopo da verificação**.
3. Clique no botão **Configurar**.

   A janela **Configurações da verificação por demanda** é exibida.
4. Clique no botão **Configurações**.
5. Selecione a guia **Ações**.
6. Selecione a ação a ser executada em objetos infectados e outros objetos detectados:
   - **Somente notificações**.
   - **Desinfectar**.
   - **Desinfectar. Remover se a desinfecção falhar**.
   - **Remover**.
   - **Executar ação recomendada**.
7. Selecione a ação a ser executada em objetos possivelmente infectados:
   - **Somente notificações**.
   - **Quarentena**.
   - **Remover**.
   - **Executar ação recomendada**.
8. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:
   a. Desmarque ou marque a caixa **Executar ações dependendo do tipo de objeto detectado**.
   b. Clique no botão **Configurações**.
   c. Na janela que se abre, selecione uma ação primária e uma ação secundária (a ser executada se a ação primária falhar) para cada tipo de objeto detectado.
   d. Clique no botão **OK**.
9. Selecione a ação a ser executada em objetos compostos incuráveis: selecione ou desmarque a caixa **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado**.
10. Clique no botão **OK**.

A nova configuração de tarefa será salva.

Configurar o desempenho

Para configurar as configurações de desempenho da tarefa de Verificação por Demanda:

1. Abra a janela Propriedades: Verificação por demanda.
2. Selecione a guia **Escopo da verificação**.
3. Clique no botão **Configurar**.

   A janela **Configurações da verificação por demanda** é exibida.
4. Clique no botão **Configurações**.
5. Selecione a guia **Desempenho**.
6. No bloco **Exclusões**:
   - Desmarque ou marque a caixa de seleção **Excluir arquivos**.
   - Desmarque ou marque a caixa **Não detectar**.
   - Clique no botão **Editar** de cada configuração para adicionar exclusões.
7. No bloco **Configurações avançadas**:
   - **Parar a verificação se demorar mais que (s)**
   - **Não verificar objetos compostos com mais de (MB)**
   - **Usar a tecnologia iSwift**
   - **Usar a tecnologia iChecker**
8. Clique no botão **OK**.

A nova configuração de tarefa será salva.

Configuração da Verificação de Unidades Removíveis

Para configurar a verificação das unidades removíveis após a conexão ao dispositivo protegido:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.

   Na janela **Propriedades: <Nome da política>**, selecione a seção **Suplementar**.
5. Clique no botão **Configurações** na subseção **Verificação de unidades removíveis**.

   A janela **Verificação de unidades removíveis** é exibida.
6. No bloco **Verificar ao conectar**, faça o seguinte:

- Marque a caixa de seleção **Verificar unidades removíveis ao conectar via USB**, se desejar que o Kaspersky Embedded Systems Security for Windows 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 desejadas para as tarefas de Verificação de Unidades Removíveis.

7. Clique no botão **OK**.

As configurações específicas são salvas e aplicadas.

Configuração da tarefa de Monitor de Comparação de Integridade de Arquivos

Para configurar a tarefa de grupo do Monitor de Comparação de Integridade de Arquivos:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados** e selecione 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.

4. Abra a janela **Propriedades: <Nome da tarefa>** usando 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**.

   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 **Escopo da verificação**, faça o seguinte:

   a. Para incluir a pasta no escopo da tarefa do Monitor de Comparação de Integridade de Arquivos:

      1. Clique no botão **Adicionar**.

         A janela **Propriedades da área de verificação** é exibida.

      2. Marque ou desmarque a caixa de seleção **Verificar esta área**.

      3. Clique no botão **Procurar** para especificar a pasta que deseja incluir no escopo da tarefa do Monitor de Comparação de Integridade de Arquivos.

      4. Marque ou desmarque a caixa de seleção **Verificar também as subpastas**, se desejar incluir todas as subpastas no escopo da tarefa do Monitor de Comparação de Integridade de Arquivos.

   b. Para incluir ou excluir a pasta adicionada anteriormente ao escopo da tarefa do Monitor de Comparação de Integridade de Arquivos, marque ou desmarque a caixa de seleção à esquerda do caminho da pasta na

tabela **Escopo da verificação**.

c. Para excluir a pasta adicionada anteriormente ao escopo da tarefa do Monitor de Comparação de Integridade de Arquivos, selecione esta pasta na tabela **Escopo da verificação** e clique no botão **Excluir**.

6. Configure a programação da tarefa na seção **Agendamento** (é possível configurar uma programação 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 executar a 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 as definições das configurações nessas seções, consulte a *Ajuda do Kaspersky Security Center*.

9. Clique no botão **OK** na janela **Propriedades: <Nome da tarefa>**.

   As recém-definidas configurações da tarefa de grupo são salvas.

Gerenciando tarefas de Verificação por Demanda por meio do Console do Aplicativo

Nesta seção, aprenda a navegar pela interface do Console do Aplicativo e definir as configurações de tarefa em um dispositivo protegido.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das configurações da tarefa de Verificação por Demanda

Para abrir as configurações gerais da tarefa de Verificação por Demanda por meio do Console do Aplicativo:

1. Expanda o node **Verificação por demanda** na árvore do Console do Aplicativo.

2. Selecione o node secundário que corresponde à tarefa que deseja configurar.

3. No painel de resultados do node secundário, clique no link **Propriedades**.

   A janela **Configurações de tarefa** é aberta.

Abertura das configurações do escopo da tarefa de Verificação por Demanda

Para abrir a janela de configurações do escopo da verificação por meio do Console do Aplicativo:

1. Expanda o node **Verificação por demanda** na árvore do Console do Aplicativo.
2. Selecione o node secundário que corresponde a uma tarefa de Verificação por Demanda que deseja configurar.
3. No painel de resultados do node selecionado, clique no link **Configurar o escopo da verificação**.

   A janela **Configurações do escopo da verificação** é exibida.

Criação e configuração de uma tarefa de Verificação por Demanda

É possível criar tarefas personalizadas para um único dispositivo protegido no node **Verificação por demanda**. Tarefas personalizadas não podem ser criadas nos outros componentes funcionais no Kaspersky Embedded Systems Security for Windows.

Para criar e configurar uma nova tarefas de Verificação por Demanda:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Verificação por demanda**.
2. Selecione **Adicionar tarefa**.

   A janela **Adicionar tarefa** é exibida.
3. Defina as seguintes configurações da tarefa:

   - **Nome** – nome da tarefa com no máximo 100 caracteres. Pode conter quaisquer símbolos, exceto **" * < > & \ : |**.

     Você não pode salvar uma tarefa ou configurar uma nova tarefa nas guias **Agendamento**, **Avançado** e **Executar como** se o nome da tarefa não for especificado.

   - **Descrição** – informações adicionais sobre a tarefa, com no máximo 2.000 caracteres. Essas informações serão exibidas na janela de propriedades de tarefa.
   - **Usar o analisador heurístico**.
   - **Executar tarefa em segundo plano**.
   - **Aplicar Zona Confiável**.
   - **Considerar tarefa como verificação de áreas críticas**.
   - **Usar a KSN para verificação**.
4. Defina as configurações de programação de inicialização da tarefa nas guias **Agendamento** e **Avançado**.
5. Na guia **Executar como**, defina as configurações para iniciar a tarefa usando permissões específicas da conta.
6. Clique no botão **OK** na janela **Adicionar tarefa**.

   É criada uma nova tarefa de Verificação por Demanda. Um nó com o nome da nova tarefa é exibido na árvore do Console do Aplicativo. A operação é registrada no log de auditoria do sistema.

7. Caso seja necessário, no painel de resultados do node selecionado, selecione **Configurar o escopo da verificação**.

   A janela **Configurações do escopo da verificação** é exibida.

8. Na árvore ou lista de recursos de arquivos do dispositivo protegido, selecione os nodes ou itens que deseja incluir no escopo da verificação.

9. Selecione um dos níveis de segurança predefinidos ou defina as configurações de verificação manualmente.

10. Clique no botão **Salvar** na janela **Configurações do escopo da verificação**.

As configurações definidas são aplicadas na próxima inicialização da tarefa.

Escopo da verificação em tarefas de Verificação por Demanda

Esta seção contém informações sobre a criação e utilização de um escopo de verificação nas tarefas de Verificação por Demanda.

Configuração da visualização de recursos de arquivos de rede

Para selecionar a visualização para recursos de arquivos de rede durante a definição das configurações do escopo da verificação:

1. Abra a janela **Configurações do escopo da verificação**.

2. Abra a lista suspensa na parte esquerda superior da janela e selecione uma das seguintes opções:

   - Selecione a opção **Visualização em árvore** para exibir os recursos de arquivos de rede em uma árvore.
   - Selecione a opção **Visualização em lista** para exibir os recursos de arquivos de rede em uma lista.

   Por padrão, os recursos de arquivos de rede do dispositivo protegido são exibidos em um modo de visualização em lista.

3. Clique no botão **Salvar**.

Criando um escopo da verificação

Se estiver gerenciando o Kaspersky Embedded Systems Security for Windows remotamente no dispositivo protegido usando o Console do Aplicativo instalado na estação de trabalho do administrador, você deverá ser membro do grupo de administradores no dispositivo protegido para poder exibir suas pastas.

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

Caso modifique o escopo da verificação nas tarefas de Verificação na inicialização do sistema operacional e Verificação de áreas críticas, será possível restaurar o escopo padrão da verificação nessas tarefas reparando o próprio Kaspersky Embedded Systems Security for Windows (**Iniciar** > **Programas** > **Kaspersky Embedded Systems Security for Windows** > **Modificar ou remover o Kaspersky Embedded Systems Security for Windows**). No assistente de instalação, selecione **Reparar componentes instalados** e clique em **Avançar**. Em seguida, marque a caixa de seleção **Restaurar configurações recomendadas do aplicativo**.

O procedimento para criar um escopo da tarefa de Verificação por Demanda depende da exibição selecionada dos recursos de arquivos de rede. É possível configurar a visualização de recursos de arquivos de rede em uma árvore ou lista (visualização padrão).

Para criar um escopo da verificação usando a árvore de recursos de arquivos de rede:

1. Abra a janela **Configurações do escopo da verificação**.
2. Na seção esquerda da janela, abra a árvore de recursos de arquivos de rede para exibir todos os nodes e nós filhos.
3. Faça o seguinte:
   - Para excluir nós individuais do escopo da verificação, desmarque as caixas ao lado dos nomes destes nós.
   - Para incluir nós individuais no escopo da verificação, desmarque a caixa de seleção **Meu Computador** e faça o seguinte:
     - Se todas as unidades de um tipo específico devem ser incluídas no escopo da verificação, marque a caixa de seleção ao lado do nome do tipo de unidade requerida (por exemplo, para adicionar todas as unidades removíveis no dispositivo protegido, selecione a caixa **Unidades removíveis**).
     - Para incluir uma unidade individual de um determinado tipo no escopo da verificação, expanda o node que contém unidades desse tipo e marque a caixa de seleção ao lado do nome da unidade desejada. Por exemplo, para selecionar a unidade removível **F:**, expanda o node **Unidades removíveis** e marque a caixa de seleção da unidade **F:**.
     - Se deseja incluir somente uma única pasta ou arquivo na unidade, selecione a caixa ao lado do nome daquela pasta ou arquivo.
4. Clique no botão **Salvar**.

A janela **Configurações do escopo da verificação** será fechada. As configurações recém-definidas são salvas.

Para criar um escopo da verificação usando a lista de recursos de arquivos de rede:

1. Abra a janela **Configurações do escopo da verificação**.
2. Para incluir nós individuais no escopo da verificação, desmarque a caixa de seleção **Meu Computador** e faça o seguinte:
   a. Abra o menu de contexto no escopo da verificação clicando com o botão direito nele.
   b. No menu de contexto do botão, selecione **Adicionar escopo da verificação**.
   c. Na janela aberta **Adicionar escopo da verificação**, selecione o tipo de objeto que deseja adicionar:
      - **Escopo predefinido**, se quiser que o escopo da verificação inclua um dos escopos predefinidos no dispositivo protegido. Em seguida, na lista suspensa, selecione o escopo da verificação desejado.

- **Disco, pasta ou local de rede** – para incluir uma unidade individual, pasta ou objeto de rede no escopo da verificação. Em seguida, selecione o escopo desejado clicando no botão **Procurar**.
- **Arquivo** – para incluir um arquivo individual no escopo da verificação. Em seguida, selecione o escopo desejado clicando no botão **Procurar**.

Não é possível adicionar um objeto a um escopo da verificação se ele já tiver sido adicionado como uma exclusão do escopo da verificação.

3. Para excluir nós individuais do escopo da verificação, desmarque as caixas ao lado dos nomes destes nós ou siga as etapas a seguir:
   a. Abra o menu de contexto no escopo da verificação clicando com o botão direito nele.
   b. No menu de contexto, selecione a opção **Adicionar exclusão**.
   c. Na janela **Adicionar exclusão**, selecione um tipo de objeto que deseja adicionar como uma exclusão do escopo da verificação seguindo o procedimento usado ao adicionar um objeto ao escopo da verificação.
4. Para modificar o escopo da verificação ou uma exclusão adicionada, selecione a opção **Editar escopo** no menu de contexto do escopo necessário.
5. Para ocultar um escopo da verificação ou exclusão adicionados anteriormente na lista de recursos de arquivos de rede, selecione a opção **Remover da lista** no menu de contexto do escopo de verificação necessário.

O escopo da verificação é excluído do escopo da tarefa de Verificação por Demanda quando ele é removido da lista de recursos de arquivos de rede.

6. Clique no botão **Salvar**.

A janela **Configurações do escopo da verificação** será fechada. As configurações recém-definidas são salvas.

Incluindo objetos de rede no escopo da verificação

Unidades, pastas ou arquivos de rede podem ser adicionados ao escopo da verificação especificando seu caminho no formato UNC (Universal Naming Convention).

Você pode verificar pastas de rede na conta do sistema.

Para adicionar uma localização de rede ao escopo da verificação:

1. Abra a janela **Configurações do escopo da verificação**.
2. Abra a lista suspensa na parte esquerda superior da janela e selecione **Visualização em árvore**.
3. No menu de contexto do node **Rede**:
   - Selecione **Adicionar pasta de rede**, se deseja adicionar uma pasta de rede ao escopo da verificação.
   - Selecione **Adicionar arquivo de rede**, se deseja adicionar um arquivo de rede ao escopo da verificação.

4. Insira o caminho para a pasta ou arquivo de rede em formato UNC e pressione a tecla **ENTER**.
5. Selecione a caixa ao lado do objeto de rede adicionado recentemente para incluí-lo no escopo da verificação.
6. Se necessário, altere as configurações de segurança do objeto de rede adicionado.
7. Clique no botão **Salvar**.

As configurações da tarefa especificadas serão salvas.

Criando um escopo de verificação virtual

As unidades, pastas e arquivos virtuais podem ser incluídos no escopo da verificação para criar um escopo de verificação virtual.

Se o escopo da verificação for exibido como uma árvore de recursos do arquivo, é possível expandi-lo adicionando unidades virtuais individuais, pastas ou arquivos.

Para adicionar uma unidade virtual ao escopo da verificação:

1. Abra a janela **Configurações do escopo da verificação**.
2. Abra a lista suspensa na parte esquerda superior da janela e selecione **Visualização em árvore**.
3. Na árvore de recursos de arquivos do dispositivo protegido, abra o menu de contexto do node **Unidades virtuais**, clique em **Adicionar unidade virtual** e selecione o nome da unidade virtual da lista de nomes disponíveis.
4. Selecione a caixa ao lado da unidade adicionada para incluir a unidade no escopo da verificação.
5. Clique no botão **Salvar**.

As configurações da tarefa especificadas serão salvas.

Para adicionar uma pasta ou arquivo virtual ao escopo da verificação:

1. Abra a janela **Configurações do escopo da verificação**.
2. Abra a lista suspensa na parte esquerda superior da janela e selecione **Visualização em árvore**.
3. Na árvore de recursos de arquivos do dispositivo protegido, abra o menu de contexto do node para adicionar uma pasta ou arquivo e selecione uma das seguintes opções:
   - **Adicionar pasta virtual**, se quiser adicionar uma pasta virtual ao escopo da verificação.
   - **Adicionar arquivo virtual**, se quiser adicionar um arquivo virtual ao escopo da verificação.
4. No campo de entrada, especifique o nome da pasta ou arquivo.
5. Na linha com o nome da pasta ou arquivo, selecione a caixa de seleção para incluir essa pasta ou arquivo no escopo da verificação.
6. Clique no botão **Salvar**.

As configurações da tarefa especificadas serão salvas.

Definição das configurações de segurança

Por padrão, as tarefas de Verificação por Demanda usam configurações de segurança comuns para o escopo da verificação inteiro.

Estas configurações correspondem ao nível de segurança predefinido **Recomendado**.

Os valores padrão das configurações de segurança podem ser modificados, definindo-os como configurações comuns para todo o escopo da verificação ou como configurações diferentes para itens diferentes na lista de recursos de arquivos ou nós da árvore do dispositivo protegido.

Ao trabalhar com a árvore de recursos de arquivos de rede, as configurações de segurança definidas para o node principal selecionado são automaticamente aplicadas a todos os nodes secundários. As configurações de segurança do node principal não são aplicadas a nós filhos configurados separadamente.

Para definir manualmente as configurações de segurança:

1. Abra a janela **Configurações do escopo da verificação**.
2. Na parte esquerda da janela, selecione o node ou item cujas configurações de segurança deseja definir.

   Um modelo predefinido de configurações de segurança pode ser aplicado em um nó ou item selecionado no escopo da verificação.

   Na parte esquerda da janela, é possível selecionar a exibição de recursos de arquivos de rede, criar um escopo de verificação ou criar um escopo de proteção virtual.
3. Na parte direita da janela, execute uma das seguintes ações:
   - Na guia **Nível de segurança**, selecione o nível de segurança a ser aplicado.
   - Defina as configurações de segurança para o node ou item selecionado de acordo com seus requisitos:
     - **Geral**
     - **Ações**
     - **Desempenho**
     - **Armazenamento hierárquico**
4. Clique no botão **Salvar** na janela **Configurações do escopo da verificação**.

As novas configurações de escopo da verificação são salvas.

Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda

É possível aplicar um dos seguintes três níveis de segurança predefinidos para um nó selecionado na árvore ou lista de recursos de arquivos do dispositivo protegido: **Desempenho máximo**, **Recomendado** e **Proteção máxima**.

Para selecionar um dos níveis de segurança predefinidos:

1. Abra a janela **Configurações do escopo da verificação**.
2. Na árvore ou na lista de recursos de arquivos de rede do dispositivo protegido, selecione um nó ou item para definir o nível de segurança predefinido.
3. Certifique-se de que o node ou item selecionado seja incluído no escopo da verificação.
4. Na parte direita da janela, na guia **Nível de segurança**, selecione o nível de segurança a ser aplicado.

   A janela exibe a lista de configurações de segurança correspondentes ao nível de segurança selecionado.
5. Clique no botão **Salvar**.

   As configurações da tarefa serão salvadas e aplicadas imediatamente à tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

Definir configurações gerais de tarefas

Para definir as configurações de segurança gerais da tarefa de Verificação por Demanda:

1. Abra a janela **Configurações do escopo da verificação**.
2. Abra a guia **Geral**.
3. No grupo **Verificar objetos**, especifique os tipos objeto que deseja incluir no escopo da verificação:
   - **Objetos a serem verificados**:
     - **Todos os objetos**
     - **Objetos verificados por formato**
     - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**
     - **Objetos verificados pela lista de extensões especificada**
   - **Verificar setores de inicialização do disco e MBR**
   - **Verificar fluxos NTFS alternativos**
4. No grupo **Desempenho**, selecione ou desmarque a caixa **Verificar apenas arquivos novos e modificados**.

   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. No grupo **Verificação de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da verificação:
   - **Todos**/**Apenas novos arquivos compactados**

- **Todos**/**Apenas novos arquivos compactados SFX**
- **Todos**/**Apenas novos bancos de dados de e-mail**
- **Todos**/**Apenas novos objetos compactados**
- **Todos**/**Apenas novos e-mails sem formatação**
- **Todos**/**Apenas novos objetos OLE incorporados**

6. Clique no botão **Salvar**.

A nova configuração de tarefa será salva.

Configurar ações

Para configurar as ações em objetos infectados e outros objetos detectados da tarefa Verificação por Demanda:

1. Abra a janela **Configurações do escopo da verificação**.
2. Selecione a guia **Ações**.
3. Selecione a ação a ser executada em objetos infectados e outros objetos detectados:
   - **Somente notificações**.
   - **Desinfectar**.
   - **Desinfectar. Remover se a desinfecção falhar**Remover, caso a desinfecção falhe.
   - **Remover**.
   - **Executar ação recomendada**.
4. Selecione a ação a ser executada em objetos possivelmente infectados:
   - **Somente notificações**.
   - **Quarentena**.
   - **Remover**.
   - **Executar ação recomendada**.
5. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:
   a. Desmarque ou marque a caixa **Executar ações dependendo do tipo de objeto detectado**.
   b. Clique no botão **Configurações**.
   c. Na janela que se abre, selecione uma ação primária e uma ação secundária (a ser executada se a ação primária falhar) para cada tipo de objeto detectado.
   d. Clique no botão **OK**.

6. Selecione a ação a ser executada em objetos compostos incuráveis: selecione ou desmarque a caixa **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado**.

7. Clique no botão **Salvar**.

A nova configuração de tarefa será salva.

Configurar o desempenho

Para configurar as configurações de desempenho da tarefa de Verificação por Demanda:

1. Abra a janela **Configurações do escopo da verificação**.
2. Selecione a guia **Desempenho**.
3. No bloco **Exclusões**:
   - Desmarque ou marque a caixa de seleção **Excluir arquivos**.
   - Desmarque ou marque a caixa **Não detectar**.
   - Clique no botão **Editar** de cada configuração para adicionar exclusões.
4. No bloco **Configurações avançadas**:
   - **Parar a verificação se demorar mais que (s)**
   - **Não verificar objetos compostos com mais de (MB)**
   - **Usar a tecnologia iSwift**
   - **Usar a tecnologia iChecker**
5. Clique no botão **Salvar**.

A nova configuração de tarefa será salva.

Configuração do armazenamento hierárquico

Para configurar as ações em objetos infectados e outros objetos detectados da tarefa Verificação por Demanda:

1. Abra a janela **Configurações do escopo da verificação**.
2. Selecione a guia **Armazenamento hierárquico**.
3. Selecione a ação a ser executada nos arquivos:
   - **Não verificar**
   - **Verificar somente a parte do arquivo residente**
   - **Verificar o arquivo inteiro**

Se esta ação for selecionada, você poderá especificar as seguintes opções:

- Selecione ou desmarque a caixa **Somente se o arquivo tiver sido acessado no período especificado (dias)** e especifique o número de dias.
- Selecione ou desmarque a caixa **Não copie o arq. p/ disco rígido local, se possível**.

4. Clique no botão **Salvar**.

A nova configuração de tarefa será salva.

Verificação de unidades removíveis

Para configurar a verificação de unidades removíveis após a conexão ao dispositivo protegido no Console do Aplicativo:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Kaspersky Embedded Systems Security for Windows** e selecione a opção **Configurar verificação de unidades removíveis**.

   A janela **Verificação de unidades removíveis** é exibida.

2. No bloco **Verificar ao conectar**, faça o seguinte:

   - Marque a caixa de seleção **Verificar unidades removíveis ao conectar via USB**, se desejar que o Kaspersky Embedded Systems Security for Windows 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 desejadas para as tarefas de Verificação de Unidades Removíveis.

3. Clique no botão **OK**.

As configurações específicas são salvas e aplicadas.

Estatísticas da tarefa de Verificação por Demanda

Enquanto uma tarefa de Verificação por Demanda está sendo executada, é possível exibir informações sobre o número de objetos processados pelo Kaspersky Embedded Systems Security for Windows desde que ele foi iniciado.

Essas informações permanecem disponíveis mesmo que a tarefa seja pausada. Você pode exibir estatísticas da tarefa no log de tarefas.

Para exibir as estatísticas de uma tarefa de Verificação por Demanda:

1. Expanda o node **Verificação por demanda** na árvore do Console do Aplicativo.
2. Selecione a tarefa de Verificação por Demanda cujas estatísticas você deseja exibir.

As estatísticas de tarefas são exibidas na seção **Estatísticas** do painel de resultados do node selecionado.

Informações sobre os objetos processados pelo Kaspersky Embedded Systems Security for Windows desde que foi iniciado estão presentes na tabela abaixo.

Estatísticas da tarefa de Verificação por Demanda

Campo	Descrição
Detectado	Número total de objetos detectados pelo Kaspersky Embedded Systems Security for Windows. Por exemplo, se o Kaspersky Embedded Systems Security for Windows detectar um objeto malicioso em cinco arquivos, o valor desse campo aumentará em um.
Objetos infectados e outros detectados	O número de objetos que o Kaspersky Embedded Systems Security for Windows encontrou e classificou como infectados ou o número de arquivos de software legítimos encontrados que não foram excluídos do escopo da verificação e foram classificados como softwares legítimos que podem ser usados por intrusos para danificar o dispositivo ou os dados pessoais.
Objetos possivelmente infectados detectados	Número de objetos encontrados pelo Kaspersky Embedded Systems Security for Windows que estão possivelmente infectados.
Objetos não desinfectados	Número de objetos que o Kaspersky Embedded Systems Security for Windows não desinfectou pelos seguintes motivos: • O objeto detectado é de um tipo que não pode ser desinfectado. • Ocorreu um erro durante a desinfecção.
Objetos não movidos para a Quarentena	Número de objetos que o Kaspersky Embedded Systems Security for Windows tentou colocar na Quarentena sem sucesso devido a espaço insuficiente no disco.
Objetos não removidos	Número de objetos que o Kaspersky Embedded Systems Security for Windows tentou excluir sem sucesso, devido, por exemplo, a um bloqueio no acesso ao objeto por parte de outro aplicativo.
Objetos não verificados	Número de objetos no escopo de proteção que o Kaspersky Embedded Systems Security for Windows não verificou devido, por exemplo, ao acesso ao objeto estar bloqueado por outro aplicativo.
Objetos sem backup	Número de objetos cujas cópias o Kaspersky Embedded Systems Security for Windows tentou salvar no Backup sem sucesso, devido, por exemplo, a espaço de disco insuficiente.
Erros de processamento	Número de objetos cujo processamento resultou em um erro.
Objetos desinfectados	Número de objetos desinfectados pelo Kaspersky Embedded Systems Security for Windows.
Movidos para a Quarentena	Número de objetos colocados na Quarentena pelo Kaspersky Embedded Systems Security for Windows.
Movidos para o backup	Número objetos cujas cópias o Kaspersky Embedded Systems Security for Windows salvou no Backup.
Objetos removidos	Número de objetos removidos pelo Kaspersky Embedded Systems Security for Windows.
Objetos protegidos por senha	Número de objetos (arquivos compactados, por exemplo) que o Kaspersky Embedded Systems Security for Windows ignorou porque estavam protegidos por senha.
Objetos	Número de objetos ignorados pelo Kaspersky Embedded Systems Security for Windows

corrompidos	porque seu formato estava corrompido.
Objetos processados	Número total de objetos processados pelo Kaspersky Embedded Systems Security for Windows.

Também é possível visualizar as estatísticas da tarefa de Verificação por Demanda no log de tarefas selecionado clicando no link **Abrir log de tarefas** na seção **Gerenciamento** do painel de resultados.

Recomendamos que você processe manualmente os eventos registrados na guia **Eventos** no log de tarefas após a conclusão da tarefa.

Criação e configuração de uma tarefa do Monitor de Comparação de Integridade de Arquivos

Para criar ou configurar uma nova tarefa do Monitor de Comparação de Integridade de Arquivos:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Inspeção do sistema**.
2. Selecione a **Criar tarefa de Monitor de comparação de Integridade de Arquivos**.

   A janela **Adicionar tarefa** é exibida.
3. Na lista suspensa **Algoritmo de cálculo hash**, selecione uma das opções:
   - **MD5**
   - **SHA256**
4. Na tabela **Áreas de verificação**, faça o seguinte:
   a. Para adicionar um arquivo ou pasta no escopo da tarefa do Monitor de Comparação de Integridade de Arquivos:
      1. Clique no botão **Adicionar**.

         A janela **Propriedades da área de verificação** é exibida.
      2. Marque ou desmarque a caixa de seleção **Verificar esta área**.
      3. Clique no botão **Procurar** para especificar o arquivo ou a pasta que deseja incluir no escopo da tarefa do Monitor de Comparação de Integridade de Arquivos.
      4. Marque ou desmarque a caixa de seleção **Verificar também as subpastas**, se desejar incluir todas as subpastas no escopo da tarefa do Monitor de Comparação de Integridade de Arquivos.
      5. Clique no botão **OK**.

   b. Para alterar um arquivo ou pasta adicionado anteriormente ao escopo da tarefa do Monitor de Comparação de Integridade de Arquivos:
      1. Clique no botão **Alterar**.

         A janela **Propriedades da área de verificação** é exibida.

2. Marque ou desmarque a caixa de seleção **Verificar esta área**.

3. Clique no botão **Procurar** para especificar o arquivo ou a pasta que deseja incluir no escopo da tarefa do Monitor de Comparação de Integridade de Arquivos.

4. Marque ou desmarque a caixa de seleção **Verificar também as subpastas**, se desejar incluir ou excluir todas as subpastas do escopo da tarefa do Monitor de Comparação de Integridade de Arquivos.

5. Clique no botão **OK**.

c. Para excluir o arquivo ou pasta adicionada anteriormente ao escopo da tarefa do Monitor de Comparação de Integridade de Arquivos, selecione esse arquivo ou pasta na tabela **Áreas de verificação** e clique no botão **Remover**.

5. Defina as configurações de programação de inicialização da tarefa nas guias **Agendamento** e **Avançado**.

6. Na guia **Executar como**, defina as configurações para iniciar a tarefa usando permissões específicas da conta.

7. Clique no botão **OK** na janela **Adicionar tarefa**.

   Uma nova tarefa personalizada do Monitor de Comparação de Integridade de Arquivos está criada. Um nó com o nome da nova tarefa é exibido na árvore do Console do Aplicativo. A operação é registrada no log de auditoria do sistema.

Para abrir as configurações da tarefa do Monitor de Comparação de Integridade de Arquivos:

1. Na árvore do Console do Aplicativo, expanda o node **Inspeção do sistema**.

2. Selecione o node secundário que corresponde à tarefa que deseja configurar.

3. No painel de resultados do node secundário, clique no link **Propriedades**.

   A janela **Configurações de tarefa** é aberta.

Gerenciamento das tarefas de Verificação por Demanda por meio do Plug-in da Web

Nesta seção, saiba como navegar pela interface do Plug-in da Web para os dispositivos protegidos na rede.

Abertura do assistente da tarefa de Verificação por Demanda

Para começar a criar uma nova tarefa de Verificação por Demanda local:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.

2. Clique na guia **Grupos** para selecionar o grupo de administração ao qual o dispositivo protegido pertence.

3. Clique no nome do dispositivo protegido.

4. Na janela **<Nome do dispositivo>** que é exibida, selecione a guia **Tarefas**.

5. Clique no botão **Adicionar**.

   A janela **Assistente de Nova Tarefa** será aberta.

6. Na lista suspensa **Aplicativo**, selecione **Kaspersky Embedded Systems Security for Windows**.
7. Na lista suspensa **Tipo de tarefa**, selecione a tarefa de **Verificação por demanda**.
8. Clique no botão **Avançar**.

Defina as configurações da tarefa conforme necessário.

Para começar a criar uma nova tarefa de Verificação por Demanda de grupo:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Tarefas**.
2. Clique na guia **Grupos** para selecionar o grupo de administração para o qual deseja criar uma tarefa.
3. Clique no botão **Adicionar**.
   A janela **Assistente de Nova Tarefa** será aberta.
4. Na lista suspensa **Aplicativo**, selecione **Kaspersky Embedded Systems Security for Windows**.
5. Na lista suspensa **Tipo de tarefa**, selecione a tarefa de **Verificação por demanda**.
6. Clique no botão **Avançar**.

Defina as configurações da tarefa conforme necessário.

Para começar a criar uma nova tarefa de Verificação por Demanda para um grupo personalizado:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Seleções de dispositivos**.
2. Marque a seleção para a qual você deseja criar uma tarefa.
3. Clique no botão **Iniciar**.
4. Na janela **Resultados da seleção**, selecione os dispositivos para os quais você deseja criar uma tarefa.
5. Clique no botão **Nova tarefa**.
6. Na lista suspensa **Aplicativo**, selecione **Kaspersky Embedded Systems Security for Windows**.
7. Na lista suspensa **Tipo de tarefa**, selecione a tarefa de **Verificação por demanda**.
8. Clique no botão **Avançar**.

Defina as configurações da tarefa conforme necessário.

Para configurar uma tarefa de Verificação por Demanda existente:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Tarefas**.
2. Clique no nome da tarefa na lista de tarefas do Kaspersky Security Center.

A janela **<Nome da tarefa>** é exibida.

Abertura das propriedades da tarefa de Verificação por Demanda

Para abrir as propriedades do aplicativo para a tarefa de Verificação por Demanda para um único dispositivo protegido:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.
2. Clique na guia **Grupos** para selecionar o grupo de administração ao qual o dispositivo protegido pertence.
3. Clique no nome do dispositivo protegido.
4. Na janela **<Nome do dispositivo>** que é exibida, selecione a guia **Tarefas**.
5. Na lista de tarefas criadas para o dispositivo, selecione a tarefa de Verificação por Demanda que você criou.
6. Abra na guia **Configurações do aplicativo**.

Configuração do escopo da verificação da tarefa

Para configurar o escopo da verificação de uma tarefa de Verificação por Demanda existente:

1. Abra as propriedades da tarefa de Verificação por Demanda.
2. Selecione a seção **Escopo da verificação**.
3. Execute uma das seguintes ações:
   - Clique no botão **Adicionar** para adicionar uma nova regra.
   - Selecione uma regra existente e clique no botão **Editar**.

   A janela **Editar escopo** é aberta.
4. Mude o botão de alternância para **Ativa** e selecione um tipo de objeto.
5. Na seção **Proteção de objetos**, defina as seguintes configurações:
   - **Modo de proteção de objetos**:
     - **Todos os objetos**
     - **Objetos verificados por formato**
     - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**
     - **Objetos verificados pela lista de extensões especificada**
   - **Subpastas**
   - **Subarquivos**

- Verificar setores de inicialização do disco e MBR
- Verificar fluxos NTFS alternativos
- Proteger somente arquivos novos e modificados

6. Na seção **Proteção de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da verificação:
   - Arquivos compactados
   - Arquivos compactados SFX
   - Objetos compactados
   - Bancos de dados de e-mail
   - E-mail sem formatação
   - Objetos OLE incorporados
7. Na seção **Ação a ser executada em objetos infectados e outros**, selecione a ação a ser executada em objetos infectados e outros objetos detectados:
   - Somente notificações.
   - **Desinfectar**.
   - **Desinfectar. Remover se a desinfecção falhar**Remover, caso a desinfecção falhe.
   - Remover.
   - **Recomendado**.
8. Na seção **Ação a ser executada em objetos possivelmente infectados**, selecione a ação a ser executada em objetos possivelmente infectados:
   - Somente notificações.
   - **Quarentena**.
   - Remover.
   - Recomendado.
9. Na seção **Ação a ser executada em objetos possivelmente infectados**, marque ou desmarque a caixa de seleção Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado.
10. Na seção **Exclusões**, é possível definir as seguintes configurações:
    - Desmarque ou marque a caixa de seleção Excluir arquivos.
    - Desmarque ou marque a caixa Não detectar.
11. Na seção **Configurações avançadas**, defina as seguintes configurações:

- **Parar a verificação se demorar mais que (s)**
- **Não verificar objetos compostos com mais de (MB)**
- **Usar a tecnologia iSwift**
- **Usar a tecnologia iChecker**

12. Na seção **Ação nos arquivos offline**, selecione a ação a ser executada nos arquivos:
    - **Não verificar**
    - **Verificar somente a parte do arquivo residente**
    - **Verificar o arquivo inteiro**

      Se esta ação for selecionada, você poderá especificar as seguintes opções:

      - Selecione ou desmarque a caixa **Somente se o arquivo tiver sido acessado no período especificado (dias)** e especifique o número de dias.
      - Selecione ou desmarque a caixa **Não copiar o arq. p/ disco rígido local, se possível**.
13. Clique no botão **OK**.

Definição das configurações da tarefa

Para configurar uma tarefa de Verificação por Demanda existente:

1. Abra as propriedades da tarefa de Verificação por Demanda.
2. Selecione a seção **Opções**.
3. Desmarque ou marque a caixa de seleção **Usar o Analisador heurístico**.
4. Caso seja necessário, selecione o nível de análise utilizando a lista suspensa **Nível de análise heurística**.
5. Na seção **Integração com outros componentes**, defina as seguintes configurações:
    - Selecione a caixa **Aplicar Zona Confiável** se desejar excluir os objetos adicionados à lista da Zona Confiável do escopo da verificação da tarefa.
    - Marque a caixa de seleção **Usar a KSN para verificação** se quiser usar os serviços na nuvem da Kaspersky Security Network para a tarefa.
    - Para atribuir a prioridade *Baixa* ao processo de trabalho onde a tarefa será executada, marque a caixa de seleção **Executar tarefa em segundo plano**.

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

    - Para utilizar uma tarefa criada como uma tarefa de Verificação de Áreas Críticas, marque a caixa de seleção **Considerar tarefa como verificação de áreas críticas**.

Zona confiável

Essa seção fornece informações sobre a Zona Confiável no Kaspersky Embedded Systems Security for Windows, bem como instruções sobre como adicionar objetos à Zona Confiável ao executar tarefas.

Sobre a Zona Confiável

A Zona Confiável é uma lista de exclusões do escopo de proteção ou verificação que é possível gerar e aplicar às tarefas de Verificação por Demanda e Proteção de Arquivos em Tempo Real, recém-criadas como tarefas de Verificação por Demanda personalizadas e todas as tarefas de Verificação por Demanda do sistema, exceto para a tarefa de Verificação da Quarentena.

A Zona Confiável é aplicada às tarefas de Proteção de Arquivos em Tempo Real e de Verificação por Demanda por padrão.

A lista de regras para gerar a Zona Confiável pode ser exportada para um arquivo de configuração XML para que seja importado para o Kaspersky Embedded Systems Security for Windows sendo executado em outro dispositivo protegido.

Processos confiáveis

Aplica-se a tarefas de Proteção de Arquivo em Tempo Real.

Alguns aplicativos no dispositivo protegido podem ficar instáveis se os arquivos que acessam forem interceptados pelo Kaspersky Embedded Systems Security for Windows. Esses aplicativos incluem, por exemplo, controladores de domínio do sistema.

Para não afetar a operação desses aplicativos, você pode desativar a proteção de arquivos acessados pelos processos de execução desses aplicativos (dessa forma criando uma lista de processos confiáveis na Zona Confiável).

A Microsoft Corporation recomenda excluir alguns arquivos do sistema operacional Microsoft Windows e arquivos de aplicativo da Microsoft da Proteção de Arquivos em Tempo Real como programas que não podem ser infectados. Os nomes de alguns deles estão listados no site da Microsoft (código do artigo: KB822158).

Você pode ativar ou desativar o uso de processos confiáveis na Zona Confiável.

Se um arquivo executável for modificado, por exemplo, por uma atualização, o Kaspersky Embedded Systems Security for Windows o excluirá da lista de processos confiáveis.

O aplicativo não usa o caminho do arquivo em um dispositivo protegido para confiar no processo. O caminho para o arquivo no dispositivo protegido é usado somente para procurar o arquivo, calcular uma soma de verificação e fornecer ao usuário informações sobre a origem do arquivo executável.

Operações de backup

Aplica-se a tarefas de Proteção do Computador em Tempo Real.

Quando os dados armazenados nos discos rígidos passam por backup em dispositivos externos, você pode desativar a proteção de objetos que são acessados durante as operações de backup. O Kaspersky Embedded Systems Security for Windows verificará os objetos que o aplicativo de backup abre para leitura com o atributo FILE_FLAG_BACKUP_SEMANTICS.

Exclusões

- Aplicável às tarefas de Proteção de Arquivos em Tempo Real.
- Todos os objetos detectáveis nas áreas especificadas do dispositivo protegido.
- Objetos detectáveis especificados por nome ou máscara de nome em todo o escopo da proteção ou da verificação.

Gerenciamento da Zona Confiável por meio do Plug-in de Administração

Nesta seção, saiba como navegar pela interface do Plug-in de Administração e configurar a Zona Confiável para um ou todos os dispositivos protegidos da rede.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das configurações da política de Zona Confiável

Para abrir a Zona Confiável por meio da política do Kaspersky Security Center:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Suplementar**.
6. Clique no botão **Configurações** na subseção **Zona Confiável**.

   A janela **Zona Confiável** é exibida.

Configure a Zona Confiável conforme necessário.

Se um dispositivo protegido estiver sendo gerenciado por uma política ativa do Kaspersky Security Center e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas por meio do Console do Aplicativo.

Abertura da janela de propriedades da Zona Confiável

Para configurar a Zona Confiável na janela de propriedades do Aplicativo:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Dispositivos**.
4. Abra a janela **Propriedades: <Nome do dispositivo protegido>** usando uma das seguintes maneiras:
   - Clique duas vezes no nome do dispositivo protegido.
   - Abra o menu de contexto do nome do dispositivo protegido e selecione o item **Propriedades**.

   A janela **Propriedades: <Nome do dispositivo protegido>** é exibida.
5. Na seção **Aplicativos**, selecione **Kaspersky Embedded Systems Security 3.3 for Windows**.
6. Clique no botão **Propriedades**.

   A janela de **Configurações do aplicativo** do **Kaspersky Embedded Systems Security 3.3 for Windows** é exibida.
7. Selecione a seção **Suplementar**.
8. Clique no botão **Configurações** na subseção **Zona Confiável**.

   A janela **Zona Confiável** é exibida.

Configure a Zona Confiável conforme necessário.

Configuração da Zona Confiável por meio do Plug-in de Administração

Para definir as configurações da Zona Confiável:

1. Na guia **Exclusões**, especifique os objetos a serem ignorados pelo Kaspersky Embedded Systems Security for Windows durante a execução da tarefa.
2. Na guia **Processos confiáveis**, especifique os processos a serem ignorados pelo Kaspersky Embedded Systems Security for Windows durante a execução da tarefa.
3. Aplique a máscara de não vírus.

Adição de exclusões

Para adicionar uma exclusão na Zona Confiável na política do Kaspersky Security Center:

1. Abra a janela **Zona Confiável**.
2. Na guia **Exclusões**, especifique os objetos a serem ignorados pelo Kaspersky Embedded Systems Security for Windows durante a verificação e proteção:
   - Para criar exclusões recomendadas, clique no botão Adicionar exclusões recomendadas.
   - Para importar exclusões pré-configuradas, clique no botão **Importar** e, na janela aberta, selecione o arquivo de configuração no formato XML armazenado no dispositivo.

     As exclusões do arquivo XML serão adicionadas à lista de exclusão.
   - Para especificar manualmente as condições sob as quais um arquivo será considerado confiável, clique no botão **Adicionar** e prossiga para as próximas etapas.

     A janela **Parâmetros da regra de exclusão** é exibida.
3. Caso tenha clicado no botão **Adicionar**, na seção **O objeto não será verificado se as seguintes condições forem atendidas**, especifique os objetos que deseja excluir do escopo da proteção/verificação e os objetos que deseja excluir entre os objetos detectáveis:
   - Se você desejar excluir um objeto do escopo da proteção ou verificação:
     a. Marque a caixa de seleção **Objeto excluído da verificação**.
     b. Clique no botão **Editar**.

        A janela **Objeto a ser excluído da verificação** será aberta.
     c. Especifique o objeto que você quer excluir do escopo da verificação.

        Ao especificar os objetos, é possível usar máscaras de nomes (por meio dos caracteres ? e *) e todos os tipos de variáveis de ambiente. O processamento de variáveis de ambiente (substituindo variáveis por seus valores) é realizado pelo Kaspersky Embedded Systems Security for Windows ao iniciar uma tarefa ou ao aplicar novas configurações a uma tarefa em execução (não aplicável às tarefas de Verificação por Demanda). O Kaspersky Embedded Systems Security for Windows processa variáveis de ambiente na conta usada para iniciar a tarefa. Para mais informações sobre variáveis de ambiente, consulte a base de dados de conhecimento da Microsoft.

     d. Clique no botão **OK**.
     e. Selecione a caixa **Aplicar a subpastas** se você quiser excluir todos os arquivos e pastas filhos do objeto especificado do escopo de proteção ou verificação.
   - Se deseja especificar o nome de um objeto detectável:
     a. Marque a caixa de seleção **Objetos excluídos da detecção**.
     b. Clique no botão **Editar**.

        A janela **Objetos a serem excluídos da detecção** é exibida.

c. Especifique o nome ou a máscara do nome do objeto detectável de acordo com a classificação da Enciclopédia de Vírus.

d. Clique no botão **Adicionar**.

e. Clique no botão **OK**.

4. No bloco **Exclusão do escopo de uso**, marque as caixas de seleção ao lado dos nomes das tarefas para as quais a exclusão deve ser aplicada.

5. Clique no botão **OK**.

A exclusão é exibida na lista na guia **Exclusões** da janela **Zona Confiável**.

Adição de processos confiáveis usando o Plug-in de Administração

Para adicionar um ou mais processos na lista de processos confiáveis com o uso do Plug-in de Administração:

1. Abra a janela **Zona Confiável**.

2. Selecione a guia **Processos confiáveis**.

3. Marque a caixa de seleção Não verificar operações de backup de arquivos para ignorar a verificação de operações de leitura de arquivos.

4. Marque a caixa de seleção **Não verificar a atividade dos arquivos dos processos especificados** para ignorar a verificação de operações de arquivos de processos confiáveis.

5. Para adicionar processos à lista de processos confiáveis, execute uma das seguintes ações:

   - Para importar processos confiáveis pré-configurados, clique no botão **Importar** e, na janela que se abre, selecione o arquivo de configuração no formato XML armazenado no dispositivo.

     Os processos do arquivo XML serão adicionados à lista de processos confiáveis.

   - Para especificar manualmente os processos, clique no botão **Adicionar** e prossiga para as próximas etapas.

6. Caso tenha clicado no botão **Adicionar**, no menu de contexto do botão, selecione uma das opções:

   - **Múltiplos processos**.

     Na janela **Adicionar processos confiáveis**, configure o seguinte:

     a. **Use o caminho inteiro do processo no disco para saber se é confiável**.

     b. **Use o hash de arquivo do processo para saber se é confiável**.

     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. No bloco **Exclusão do escopo de uso**, marque as caixas de seleção ao lado dos nomes das tarefas para as quais deseja aplicar as exclusões.

h. Clique no botão **OK**.

A conta em que a tarefa Proteção de Arquivos em Tempo Real é executada precisa ter direitos de administrador no dispositivo com o Kaspersky Embedded Systems Security for Windows instalado para que seja possível visualizar a lista de processos ativos. Você pode ordenar processos na lista de processos ativos por nome de arquivo, identificador do processo (PID) ou caminho para o arquivo executável do processo no dispositivo protegido. Note que é possível selecionar processos em execução clicando no botão **Processos** usando apenas o Console do Aplicativo em um dispositivo protegido, ou nas configurações do host especificado por meio do Kaspersky Security Center.

- **Um processo com base no nome e caminho do arquivo**.

  Na janela **Adicionar processo**, faça o seguinte:

  a. Insira um caminho para um arquivo executável (inclusive o nome do arquivo).

  Ao especificar os objetos, é possível usar máscaras de nomes (por meio dos caracteres `?` e `*`) e todos os tipos de variáveis de ambiente. O processamento de variáveis de ambiente (substituindo variáveis por seus valores) é realizado pelo Kaspersky Embedded Systems Security for Windows ao iniciar uma tarefa ou ao aplicar novas configurações a uma tarefa em execução (não aplicável às tarefas de Verificação por Demanda). O Kaspersky Embedded Systems Security for Windows processa variáveis de ambiente na conta usada para iniciar a tarefa. Para mais informações sobre variáveis de ambiente, consulte a base de dados de conhecimento da Microsoft.

  b. No bloco **Exclusão do escopo de uso**, marque as caixas de seleção ao lado dos nomes das tarefas para as quais deseja aplicar as exclusões.

  c. Clique no botão **OK**.

- **Um processo com base nas propriedades do objeto**.

  Na janela **Adição de processo confiável**, configure o seguinte:

  a. Clique no botão **Procurar** para selecionar um processo.

  b. Use o caminho inteiro do processo no disco para saber se é confiável.

  c. Use o hash de arquivo do processo para saber se é confiável.

  d. No bloco **Exclusão do escopo de uso**, marque as caixas de seleção ao lado dos nomes das tarefas para as quais deseja aplicar as exclusões.

  e. Clique no botão **OK**.

Para adicionar o processo selecionado à lista de processos confiáveis, pelo menos um critério de confiança deve ser selecionado.

Caso um processo tenha sido tornado confiável para a tarefa Controle de Inicialização de Aplicativos e um pacote de distribuição confiável tenha sido criado pelo arquivo executável desse processo nas configurações da tarefa, as configurações da Zona Confiável têm uma prioridade mais alta. O Kaspersky Embedded Systems Security for Windows considera o processo confiável, mas bloqueia a execução do arquivo executável desse processo.

7. Na janela **Zona 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 a verificação de arquivos de software e recursos da web legítimos que podem ser considerados perigosos. 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 for Windows aplicará as ações especificadas nas configurações da tarefa para os recursos de software nesta categoria.

Para aplicar a máscara de não vírus:

1. Abra a janela **Zona Confiável**.
2. Na guia **Exclusões**, na coluna **Objetos a detectar**, role a lista e selecione a linha com não é um vírus:*, caso a caixa de seleção esteja desmarcada.
3. Clique no botão **OK**.

A nova configuração é aplicada.

Gerenciamento da Zona Confiável por meio do Console do Aplicativo

Nesta seção, aprenda como navegar pela interface do Console do Aplicativo e configurar a Zona Confiável em um dispositivo protegido.

Aplicar Zona Confiável a tarefas no Console do Aplicativo

Por padrão, a Zona Confiável é aplicada à tarefa de Proteção de Arquivos em Tempo Real, tarefas de Verificação por Demanda personalizadas recém-criadas e em todas as tarefas de Verificação por Demanda do sistema, exceto a tarefa de Verificação da Quarentena.

Após a Zona Confiável ser ativada ou desativada, as exclusões especificadas serão aplicadas imediatamente ou deixarão de ser aplicadas a tarefas em execução.

Para ativar ou desativar o uso da Zona Confiável em tarefas do Kaspersky Embedded Systems Security for Windows:

1. Na árvore do Console do Aplicativo, abra o menu de contexto da tarefa para a qual deseja configurar o uso da Zona Confiável.
2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é aberta.
3. Na janela aberta, selecione a guia **Geral** e execute uma das seguintes ações:

   - Para aplicar a zona confiável à tarefa, selecione a caixa **Aplicar Zona Confiável**.
   - Para desativar a Zona Confiável na tarefa, desmarque a caixa de seleção **Aplicar Zona Confiável**.
4. Se desejar definir as configurações da Zona Confiável, clique no link no nome da caixa de seleção **Aplicar Zona Confiável**.

   A janela **Zona Confiável** é exibida.

   Na janela **Zona Confiável**, configure as exclusões e os processos confiáveis e clique em **OK**.
5. Clique no botão **OK** na janela **Configurações de tarefa** para salvar as alterações.

Configuração da Zona Confiável no Console do Aplicativo

Para definir as configurações da Zona Confiável:

1. Especifique os objetos a serem ignorados pelo Kaspersky Embedded Systems Security for Windows durante a execução da tarefa na guia **Exclusões**.
2. Especifique os processos a serem ignorados pelo Kaspersky Embedded Systems Security for Windows durante a execução da tarefa na guia **Processos confiáveis**.
3. Aplicar a Zona Confiável para as tarefas do aplicativo.
4. Aplique a máscara de não vírus.

Adição de uma exclusão à Zona Confiável

Para adicionar uma exclusão manualmente à Zona Confiável por meio do Console do Aplicativo:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Kaspersky Embedded Systems Security for Windows**.
2. Selecione a opção de menu **Configurar a Zona Confiável**.

   A janela **Zona Confiável** é exibida.
3. Selecione a guia **Exclusões**.
4. Especifique os objetos a serem ignorados pelo Kaspersky Embedded Systems Security for Windows durante a verificação e proteção:

- Para importar exclusões pré-configuradas, clique no botão **Importar** e, na janela aberta, selecione o arquivo de configuração no formato XML armazenado no dispositivo.

  As exclusões do arquivo XML serão adicionadas à lista de exclusão.

- Para especificar manualmente as condições sob as quais um arquivo será considerado confiável, clique no botão **Adicionar** e prossiga para as próximas etapas.

  A janela **Parâmetros da regra de exclusão** é exibida.

5. Caso tenha clicado no botão **Adicionar**, na seção **O objeto não será verificado se as seguintes condições forem atendidas**, especifique os objetos que deseja excluir do escopo da proteção/verificação e os objetos que deseja excluir entre os objetos detectáveis:

   - Se você desejar excluir um objeto do escopo da proteção ou verificação:

     a. Marque a caixa de seleção **Objeto excluído da verificação**.

     b. Clique no botão **Editar**.

        A janela **Objeto a ser excluído da verificação** será aberta.

     c. Especifique o objeto que você quer excluir do escopo da verificação.

        > Ao especificar os objetos, é possível usar máscaras de nomes (por meio dos caracteres ? e *) e todos os tipos de variáveis de ambiente. O processamento de variáveis de ambiente (substituindo variáveis por seus valores) é realizado pelo Kaspersky Embedded Systems Security for Windows ao iniciar uma tarefa ou ao aplicar novas configurações a uma tarefa em execução (não aplicável às tarefas de Verificação por Demanda). O Kaspersky Embedded Systems Security for Windows processa variáveis de ambiente na conta usada para iniciar a tarefa. Para mais informações sobre variáveis de ambiente, consulte a base de dados de conhecimento da Microsoft.

     d. Clique no botão **OK**.

     e. Selecione a caixa **Aplicar a subpastas** se você quiser excluir todos os arquivos e pastas filhos do objeto especificado do escopo de proteção ou verificação.

   - Se deseja especificar o nome de um objeto detectável:

     a. Marque a caixa de seleção **Objetos excluídos da detecção**.

     b. Clique no botão **Editar**.

        A janela **Objetos a serem excluídos da detecção** é exibida.

     c. Especifique o nome ou a máscara do nome do objeto detectável de acordo com a classificação da Enciclopédia de Vírus.

     d. Clique no botão **Adicionar**.

     e. Clique no botão **OK**.

6. No bloco **Exclusão do escopo de uso**, marque as caixas de seleção ao lado dos nomes das tarefas para as quais a exclusão deve ser aplicada.

7. Clique no botão **OK**.

A exclusão é exibida na lista na guia **Exclusões** da janela **Zona Confiável**.

Adição de processos confiáveis usando o Console do Aplicativo

Você pode adicionar um processo à lista de processos confiáveis usando um dos seguintes métodos:

- Selecione o processo na lista de processos em execução no dispositivo protegido.
- Selecione o arquivo executável de um processo, independentemente de o processo estar ou não em execução no momento.

> Se o arquivo executável de um processo tiver sido modificado, o Kaspersky Embedded Systems Security for Windows excluirá esse processo da lista de processos confiáveis.

Para adicionar um ou mais processos na lista de processos confiáveis com o uso do Console do Aplicativo:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Kaspersky Embedded Systems Security for Windows**.
2. Selecione a opção de menu **Configurar a Zona Confiável**.

   A janela **Zona Confiável** é exibida.
3. Selecione a guia **Processos confiáveis**.
4. Marque a caixa de seleção **Não verificar operações de backup de arquivos** para ignorar a verificação de operações de leitura de arquivos.
5. Marque a caixa de seleção **Não verificar a atividade dos arquivos dos processos especificados** para ignorar a verificação de operações de arquivos de processos confiáveis.
6. Para adicionar processos à lista de processos confiáveis, execute uma das seguintes ações:
   - Para importar processos confiáveis pré-configurados, clique no botão **Importar** e, na janela que se abre, selecione o arquivo de configuração no formato XML armazenado no dispositivo.

     Os processos do arquivo XML serão adicionados à lista de processos confiáveis.
   - Para especificar manualmente os processos, clique no botão **Adicionar** e prossiga para as próximas etapas.
7. Caso tenha clicado no botão **Adicionar**, no menu de contexto do botão, selecione uma das opções:
   - **Múltiplos processos**.

     Na janela **Adicionar processos confiáveis**, configure o seguinte:

     a. **Use o caminho inteiro do processo no disco para saber se é confiável**.

     b. **Use o hash de arquivo do processo para saber se é confiável**.

     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. No bloco **Exclusão do escopo de uso**, marque as caixas de seleção ao lado dos nomes das tarefas para as quais deseja aplicar as exclusões.

h. Clique no botão **OK**.

A conta em que a tarefa Proteção de Arquivos em Tempo Real é executada precisa ter direitos de administrador no dispositivo com o Kaspersky Embedded Systems Security for Windows instalado para que seja possível visualizar a lista de processos ativos. Você pode ordenar processos na lista de processos ativos por nome de arquivo, identificador do processo (PID) ou caminho para o arquivo executável do processo no dispositivo protegido. Note que é possível selecionar processos em execução clicando no botão **Processos** usando apenas o Console do Aplicativo em um dispositivo protegido, ou nas configurações do host especificado por meio do Kaspersky Security Center.

- **Um processo com base no nome e caminho do arquivo**.

  Na janela **Adicionar processo**, faça o seguinte:

  a. Insira um caminho para um arquivo executável (inclusive o nome do arquivo).

  Ao especificar os objetos, é possível usar máscaras de nomes (por meio dos caracteres `?` e `*`) e todos os tipos de variáveis de ambiente. O processamento de variáveis de ambiente (substituindo variáveis por seus valores) é realizado pelo Kaspersky Embedded Systems Security for Windows ao iniciar uma tarefa ou ao aplicar novas configurações a uma tarefa em execução (não aplicável às tarefas de Verificação por Demanda). O Kaspersky Embedded Systems Security for Windows processa variáveis de ambiente na conta usada para iniciar a tarefa. Para mais informações sobre variáveis de ambiente, consulte a base de dados de conhecimento da Microsoft.

  b. No bloco **Exclusão do escopo de uso**, marque as caixas de seleção ao lado dos nomes das tarefas para as quais deseja aplicar as exclusões.

  c. Clique no botão **OK**.

- **Um processo com base nas propriedades do objeto**.

  Na janela **Adição de processo confiável**, configure o seguinte:

  a. Clique no botão **Procurar** para selecionar um processo.

  b. Use o caminho inteiro do processo no disco para saber se é confiável.

  c. Use o hash de arquivo do processo para saber se é confiável.

  d. No bloco **Exclusão do escopo de uso**, marque as caixas de seleção ao lado dos nomes das tarefas para as quais deseja aplicar as exclusões.

  e. Clique no botão **OK**.

Para adicionar o processo selecionado à lista de processos confiáveis, pelo menos um critério de confiança deve ser selecionado.

Caso um processo tenha sido tornado confiável para a tarefa Controle de Inicialização de Aplicativos e um pacote de distribuição confiável tenha sido criado pelo arquivo executável desse processo nas configurações da tarefa, as configurações da Zona Confiável têm uma prioridade mais alta. O Kaspersky Embedded Systems Security for Windows considera o processo confiável, mas bloqueia a execução do arquivo executável desse processo.

8. Na janela **Zona 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 a verificação de arquivos de software e recursos da web legítimos que podem ser considerados perigosos. 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 for Windows aplicará as ações especificadas nas configurações da tarefa para os recursos de software ou da web nesta categoria.

Para aplicar a máscara de não vírus:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Kaspersky Embedded Systems Security for Windows**.
2. Selecione a opção de menu **Configurar a Zona Confiável**.

   A janela **Zona Confiável** é exibida.
3. Selecione a guia **Exclusões**.
4. Role a lista para encontrar o valor *não vírus:**.
5. Marque a caixa de seleção correspondente, se estiver desmarcada.
6. Clique no botão **OK**.

A nova configuração é aplicada.

Gerenciamento da Zona Confiável por meio do Plug-in da Web

Para configurar a Zona Confiável por meio do Plug-in da Web:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Suplementar**.
5. Clique no botão **Configurações** na subseção **Zona Confiável**.
6. Configure a Zona Confiável conforme necessário.

Prevenção de Exploits

Esta seção contém instruções sobre como definir configurações de proteção da memória do processo.

Sobre a Prevenção de Exploits

O Kaspersky Embedded Systems Security for Windows 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 ao inserir um Agente de Proteção de Processo ("Agente de Proteção") externo no processo protegido.

Um Agente de Proteção de Processo é um módulo do Kaspersky Embedded Systems Security for Windows dinamicamente carregado que é 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 encerrar o processo afetado. Pode ser necessário reiniciar o dispositivo protegido (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 for Windows 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.

Serviço de Kaspersky Security Exploit Prevention

O Serviço de Kaspersky Security Exploit Prevention é necessário no dispositivo 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 dispositivo protegido, o processo kavfswh é criado e iniciado. Ele comunica as informações sobre os processos protegidos do componente para o Agente de Proteção.

Depois que o Serviço de Kaspersky Security Exploit Prevention for interrompido, o Kaspersky Embedded Systems Security for Windows continua a proteger os processos adicionados à lista de processos protegidos. Ele também será carregado nos processos recém-adicionados e aplicará todas as técnicas disponíveis de prevenção de exploits para proteger a memória do processo.

Se o dispositivo estiver executando o sistema operacional Windows 10 ou posterior, o aplicativo não continuará protegendo processos e a memória do processo depois que o Serviço de Kaspersky Security Exploit Prevention for interrompido.

Se o Serviço de Kaspersky Security Exploit Prevention 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 executadas 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 exploração de uma vulnerabilidade em um processo crítico do sistema operacional protegido, o Kaspersky Embedded Systems Security for Windows encerrará o processo, independentemente do modo indicado nas configurações do componente de Prevenção de Exploits.

- **Somente notificações**: aplique este modo para receber informações sobre exemplos de exploits em processos protegidos usando eventos no Log de segurança.

  Se esse modo for selecionado, o Kaspersky Embedded Systems Security for Windows cria eventos para registrar em log todas as tentativas de explorar vulnerabilidades. Selecionado por padrão.

Gerenciamento da Prevenção de Exploits por meio do Plug-in de Administração

Nessa seção, saiba como navegar pela interface do Plug-in de Administração e definir as configurações do componente para um ou todos os dispositivos protegidos na rede.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das configurações de política para Prevenção de Exploits

Para abrir as configurações de Prevenção de Exploits por meio da política do Kaspersky Security Center:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Proteção do Computador em Tempo Real**.
6. Clique em **Configurações** na subseção **Prevenção de Exploits**.

   A janela **Prevenção de Exploits** é exibida.

Configure a Prevenção de Exploits conforme necessário.

Abertura da janela de propriedades de Prevenção de Exploits

Para abrir a janela Propriedades para Prevenção de Exploits:

1. Expanda o node **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Dispositivos**.
4. Abra a janela **Propriedades: <Nome do dispositivo protegido>** usando uma das seguintes maneiras:
   - Clique duas vezes no nome do dispositivo protegido.
   - Abra o menu de contexto do nome do dispositivo protegido e selecione o item **Propriedades**.

   A janela **Propriedades: <Nome do dispositivo protegido>** é exibida.
5. Na seção **Aplicativos**, selecione **Kaspersky Embedded Systems Security 3.3 for Windows**.
6. Clique no botão **Propriedades**.

   A janela de **Configurações do aplicativo** do **Kaspersky Embedded Systems Security 3.3 for Windows** é exibida.
7. Selecione a seção **Proteção do Computador em Tempo Real**.
8. Clique em **Configurações** na subseção **Prevenção de Exploits**.

   A janela **Prevenção de Exploits** é exibida.

Configure a Prevenção de Exploits conforme necessário.

Definição das configurações de proteção da memória do processo

Para definir as configurações de Prevenção de Exploit para os processos adicionados na lista de processos protegidos, execute as seguintes ações:

1. Abra a janela **Prevenção de Exploits**.
2. No bloco **Modo de prevenção de exploits**, defina as seguintes configurações:
   - **Prevenir exploits de processos vulneráveis**.
     - **Encerrar no exploit**.
     - **Somente notificações**.
3. No bloco **Ações de prevenção**, defina as seguintes configurações:
   - **Notificar sobre processos que tenham sofrido violação pelo Serviço de terminal**.
   - **Prevenir exploits de processos vulneráveis, mesmo se o Kaspersky Security Service estiver desativado**.
4. Clique no botão **OK** na janela **Prevenção de Exploits**.

O Kaspersky Embedded Systems Security for Windows salva e aplica as configurações de proteção da memória do processo definidas.

Adição de um processo ao escopo da proteção

O componente Prevenção de Exploits protege diversos 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. Abra a janela **Prevenção de Exploits**.
2. Na guia **Processos protegidos**, clique no botão **Procurar**.
   Uma janela do Microsoft Windows Explorer é exibida.
3. Selecione o processo que você deseja adicionar à lista.
4. Clique no botão **Abrir**.
   O nome de processo é exibido na linha.
5. Clique no botão **Adicionar**.
   O processo será adicionado à lista de processos protegidos.
6. Selecione o processo adicionado.
7. Clique no botão **Definir técnicas de prevenção de exploits**.
   A janela **Técnicas de prevenção de exploits** é exibida.
8. 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. Por padrão, todas as técnicas disponíveis são aplicadas a um processo.

- **Aplicar técnicas de prevenção de exploits selecionada**

  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**.

9. 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 inicializado na Área de Internet**, marque as caixas de seleção ao lado das opções para as quais deseja permitir que módulos sejam iniciados:
     - **Internet**
     - **Intranet local**
     - **URL confiável**
     - **URL restrita**
     - **Computador**

   As configurações são aplicáveis apenas ao Internet Explorer®.

10. Clique no botão **OK**.

O processo é adicionado ao escopo da proteção da tarefa.

Gerenciamento da Prevenção de Exploits por meio do Console do Aplicativo

Nesta seção, aprenda como navegar pela interface do Console do Aplicativo e definir configurações do componente em um dispositivo protegido.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface escolhida.

Abertura das configurações gerais de Prevenção de Exploits

*Para abrir a janela **Configurações de Prevenção de Exploits**:*

1. Expanda o node **Proteção de arquivos em tempo real** na árvore do Console do Aplicativo.
2. Selecione o node **Prevenção de Exploits**.
3. Na seção Processa configurações de proteção, clique no link **Propriedades**.
   A janela **Configurações de Prevenção de Exploits** é exibida.

Defina as configurações gerais para a Prevenção de Exploits conforme necessário.

Abertura das configurações de proteção de processo de Prevenção de Exploits

*Para abrir a janela ***Processa configurações de proteção**:*

1. Expanda o node **Proteção de arquivos em tempo real** na árvore do Console do Aplicativo.
2. Selecione o node **Prevenção de Exploits**.
3. Na seção Processa configurações de proteção, clique no link **Parâmetros de proteção do processo**.
   A janela Processa configurações de proteção é exibida.
4. Defina as configurações de proteção de processo para a Prevenção de Exploits conforme necessário.

Definição das configurações de proteção da memória do processo

Para adicionar um processo à lista de processos protegidos:

1. Abra a janela Configurações de Prevenção de Exploits.
2. No bloco **Modo de prevenção de exploits**, defina as seguintes configurações:
   - Prevenir exploits de processos vulneráveis.
     - Encerrar no exploit.
     - Somente notificações.
3. No bloco **Ações de prevenção**, defina as seguintes configurações:
   - Notificar sobre processos que tenham sofrido violação pelo Serviço de terminal.
   - Prevenir exploits de processos vulneráveis, mesmo se o Kaspersky Security Service estiver desativado.
4. Clique no botão **OK** na janela **Configurações de Prevenção de Exploits**.

O Kaspersky Embedded Systems Security for Windows salva e aplica as configurações de proteção da memória do processo definidas.

Adição de um processo ao escopo da proteção

O componente Prevenção de Exploits protege diversos processos por padrão. Você pode desmarcar os processos que não deseja proteger na lista de processos protegidos.

Para adicionar um processo à lista de processos protegidos:

1. Abra a janela **Processa configurações de proteção**.
2. Para adicionar um processo para protegê-lo de violação e reduzir o impacto potencial de um exploit, execute as seguintes ações:
   a. Clique no botão **Procurar**.
      A janela **Abrir** padrão do Microsoft Windows é exibida.
   b. Na janela exibida, selecione um processo que você deseja adicionar à lista.
   c. Clique no botão **Abrir**.
   d. Clique no botão **Adicionar**.
      O processo será adicionado à lista de processos protegidos.
3. Selecione um processo na lista.
4. A configuração atual é exibida na guia **Processa configurações de proteção**:
   - **Nome do processo**.
   - **Está em execução**.
   - **Técnicas de prevenção de exploits aplicadas**.
   - **Configurações de redução da superfície de ataque**.
5. Para modificar as técnicas de prevenção de exploits aplicadas ao processo, selecione a guia **Negar carregamento de módulos**.
6. 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. Por padrão, todas as técnicas disponíveis são aplicadas a um processo.
   - **Aplicar técnicas de prevenção de exploits listados 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.
7. Defina as configurações da técnica de Redução de superfície de ataque:

- No campo **Negar módulos**, insira os nomes dos módulos cuja execução pelo processo protegido será bloqueada.
- Na seção **Não negar módulos se inicializado na Área de Internet**, marque as caixas de seleção ao lado das opções para as quais deseja permitir que módulos sejam iniciados:
  - **Internet**
  - **Intranet local**
  - **URL confiável**
  - **Sites restritos**
  - **Computador**

  As configurações são aplicáveis apenas ao Internet Explorer®.

8. Clique no botão **Salvar**.

O processo é adicionado ao escopo da proteção da tarefa.

Gerenciamento da Prevenção de Exploits por meio do Plug-in da Web

Nesta seção, saiba como navegar pela interface do Plug-in da Web e definir configurações do componente em um dispositivo protegido.

Definição das configurações de proteção da memória do processo

Para definir as configurações de Prevenção de Exploit para os processos adicionados na lista de processos protegidos, execute as seguintes ações:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Proteção do Computador em Tempo Real**.
5. Clique em **Configurações** na subseção **Prevenção de Exploits**.
6. Abra a guia **Configurações de Prevenção de Exploits**.
7. No bloco **Modo de prevenção de exploits**, defina as seguintes configurações:
   - Prevenir exploits de processos vulneráveis.
     - Encerrar no exploit.

- **Somente notificações**.

8. No bloco **Ações de prevenção**, defina as seguintes configurações:
   - **Notificar sobre processos que tenham sofrido violação pelo Serviço de terminal**.
   - **Prevenir exploits de processos vulneráveis, mesmo se o Kaspersky Security Service estiver desativado**.
9. Clique no botão **OK** na janela **Prevenção de Exploits**.

O Kaspersky Embedded Systems Security for Windows salva e aplica as configurações de proteção da memória do processo definidas.

Adição de um processo ao escopo da proteção

Para definir as configurações de Prevenção de Exploit para os processos adicionados na lista de processos protegidos, execute as seguintes ações:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política que você quer configurar.
3. Na janela **<Nome da política>** que é exibida, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Proteção do Computador em Tempo Real**.
5. Clique em **Configurações** na subseção **Prevenção de Exploits**.
6. Abra a guia **Processos protegidos**.
7. Clique no botão **Adicionar**.
8. A janela **Técnicas de prevenção de exploits** é exibida.
9. Especifique o nome do processo.
10. 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. Por padrão, todas as técnicas disponíveis são aplicadas a um processo.
    - **Aplicar as técnicas de prevenção de exploits selecionadas**

      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**.
11. 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 inicializado na Área de Internet**, marque as caixas de seleção ao lado das opções para as quais deseja permitir que módulos sejam iniciados:
  - **Internet**
  - **Intranet local**
  - **URL confiável**
  - **URL restrita**
  - **Computador**

> As configurações são aplicáveis apenas ao Internet Explorer®.

12. Clique no botão **OK**.

O processo é adicionado ao escopo da proteção da tarefa.

Técnicas de prevenção de exploits

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 de instruções potencialmente perigosas (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 por meio 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.

Integração com sistemas de terceiros

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

Contadores de desempenho do Monitor do Sistema

Esta seção contém informações sobre os contadores de desempenho do Monitor do Sistema do Microsoft Windows que são registrados pelo Kaspersky Embedded Systems Security for Windows durante a instalação.

Sobre os contadores de desempenho do Kaspersky Embedded Systems Security for Windows

Os Contadores de Desempenho são um componente do Kaspersky Embedded Systems Security for Windows que pode ser usado para monitorar o desempenho do aplicativo durante a execução de tarefas de proteção do computador em tempo real. Você pode identificar gargalos durante a execução com outros aplicativos e falhas de recursos. É possível identificar configurações indesejáveis e diagnosticar travamentos do Kaspersky Embedded Systems Security for Windows.

Você pode visualizar os contadores de desempenho do Kaspersky Embedded Systems Security for Windows abrindo o console **Desempenho** na seção **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 configurações recomendadas do Kaspersky Embedded Systems Security for Windows caso os valores dos contadores excedam os limites.

Número total de solicitações negadas

Número total de solicitações negadas

Nome	Número total de solicitações negadas
Definição	Número total de solicitações de processamento de objetos feitas pelo driver de interceptação de arquivos e não foram aceitas pelos processos do aplicativo; contado a partir do momento em que o Kaspersky Embedded Systems Security for Windows foi iniciado pela última vez. O aplicativo ignora objetos para os quais as solicitações de processamento são negadas pelos processos do Kaspersky Embedded Systems Security for Windows.
Finalidade	Este contador pode ajudá-lo a detectar: • Redução da Proteção do Computador em Tempo Real porque os processos do Kaspersky Embedded Systems Security for Windows estão sobrecarregados. • Interrupção da Proteção do Computador em Tempo Real devido a falhas de triagem da interceptação de arquivos.
Valor normal / limite	0 / 1
Intervalo de	1 hora.

leitura recomendado	
Recomendações de configuração caso o valor exceda o limite	O número de solicitações de processamento negadas 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 for Windows foram totalmente carregados, portanto, o Kaspersky Embedded Systems Security for Windows não pôde verificar objetos. Para evitar ignorar objetos, aumente o número de processos do aplicativo para as tarefas de Proteção do Computador em Tempo Real. É possível usar as configurações do Kaspersky Embedded Systems Security for Windows, como o **Número de processos para a Proteção em Tempo Real**. • O número de solicitações negadas excede de forma significativa o limite crítico e continua crescendo rapidamente: a interceptação travou. O Kaspersky Embedded Systems Security for Windows não está verificando objetos quando são acessados. Reinicie o Kaspersky Embedded Systems Security for Windows.

Número total de solicitações ignoradas

Número total de solicitações ignoradas

Nome	Número total de solicitações ignoradas
Definição	O número total de solicitações de processamento de objetos feitas pelo driver de interceptação de arquivos que foram recebidas pelo Kaspersky Embedded Systems Security for Windows e não geraram eventos indicando a conclusão do processamento; esse número é contado a partir do momento em que o aplicativo foi iniciado pela última vez. Se uma solicitação de processamento de objeto é aceita por um dos processos de trabalho, mas não enviar um evento indicando a conclusão do processamento, o driver vai transferir essa solicitação para outro processo e o valor do contador **Número total de pedidos ignorados** aumentará em 1. Se o driver tiver percorrido todos os processos de trabalho e nenhum deles tiver aceitado a solicitação de processamento (todos estavam ocupados) ou não tiver enviado um evento indicando a conclusão do processamento, o Kaspersky Embedded Systems Security for Windows vai ignorar o objeto, logo, o valor do contador **Número total de pedidos ignorados** aumentará em 1.
Finalidade	Esse contador permite detectar quedas no desempenho 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	Se o contador for diferente de zero, um ou mais 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 for Windows para restaurar os fluxos offline.

Número de solicitações não processadas devido à falta de recursos do sistema

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 for Windows foi iniciado pela última vez. O Kaspersky Embedded Systems Security for Windows ignora solicitações de processamento de objetos 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 do Computador 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 for Windows precisam de mais RAM para processar solicitações. Os processos ativos de outros aplicativos podem estar usando toda a RAM disponível.

Número de solicitações enviadas para serem processadas

Número de solicitações enviadas para serem processadas

Nome	Número de solicitações enviadas para serem processadas.
Definição	O número de objetos aguardando processamento pelos processos de trabalho.
Finalidade	Esse contador pode ser usado para monitorar a carga nos processos de trabalho do Kaspersky Embedded Systems Security for Windows e o nível geral de atividade de arquivos no dispositivo protegido.
Valor normal / limite	O contador pode variar de acordo com o nível de atividade de arquivos do dispositivo protegido.
Intervalo de leitura recomendado	1 minuto.
Recomendações de configuração caso o valor exceda o limite	N/A

Número médio de fluxos de triagem de interceptação de arquivos

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 nas tarefas de Proteção do Computador em Tempo Real.
Finalidade	Esse contador pode ser usado para detectar e eliminar uma possível redução na Proteção do Computador em Tempo Real devido à carga completa nos processos do Kaspersky Embedded Systems Security for Windows.
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 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 for Windows ignore o objeto. Aumente o número de processos do Kaspersky Embedded Systems Security for Windows para as tarefas de Proteção do Computador em Tempo Real. É possível usar as configurações do Kaspersky Embedded Systems Security for Windows, como o **Número de processos para a Proteção em Tempo Real**.

Número máximo de fluxos de triagem de interceptação de arquivos

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 nas tarefas de Proteção do Computador 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 contador **Número médio de fluxos de interceptação de arquivos**, o Kaspersky Embedded Systems Security for Windows está distribuindo a carga de forma desequilibrada pelos processos em execução. Reinicie o Kaspersky Embedded Systems Security for Windows.

Número de elementos na fila de objetos infectados

Número de elementos na fila de objetos infectados

Nome	Número de elementos 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 do Computador em Tempo Real devido a possíveis falhas de triagem da interceptação de arquivos. • A sobrecarga de processos devido à distribuição não uniforme do tempo do processador entre diferentes processos de trabalho e o Kaspersky Embedded Systems Security for Windows. • Surtos de vírus.
Valor normal / limite	Esse valor pode ser diferente de zero enquanto o Kaspersky Embedded Systems Security for Windows está processando objetos infectados ou possivelmente infectados, mas regressará 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 for Windows não está processando objetos (talvez a triagem de interceptação de arquivos tenha travado). Reinicie o Kaspersky Embedded Systems Security for Windows. • Pode haver tempo insuficiente de processador para processar os objetos. Certifique-se de que o Kaspersky Embedded Systems Security for Windows obtenha tempo de processador adicional (por exemplo, reduzindo a carga de outros aplicativos no dispositivo protegido). • 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

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	Esse contador reflete a velocidade do processamento de objetos; ele pode ser usado para detectar e eliminar pontos baixos no desempenho do dispositivo protegido que ocorrem devido a atribuição de tempo de processador insuficiente aos processos do Kaspersky Embedded Systems Security for Windows ou erros na operação do Kaspersky Embedded Systems Security for Windows.
Valor normal / limite	Varia / Nº

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 for Windows e da carga no dispositivo protegido de processos de outros aplicativos. Observe o valor médio do contador por um longo período. Caso o valor médio do contador diminua, uma das seguintes situações será possível: • Os processos do Kaspersky Embedded Systems Security for Windows não têm tempo de processador suficiente para processar os objetos. Certifique-se de que o Kaspersky Embedded Systems Security for Windows obtenha tempo de processador adicional (por exemplo, reduzindo a carga de outros aplicativos no dispositivo protegido). • Ocorreu um erro no Kaspersky Embedded Systems Security for Windows (vários fluxos estão ociosos). Reinicie o Kaspersky Embedded Systems Security for Windows.

Contadores SNMP e interceptações do Kaspersky Embedded Systems Security for Windows

Esta seção contém informações sobre os contadores e interceptações do Kaspersky Embedded Systems Security for Windows.

Sobre contadores e interceptações SNMP do Kaspersky Embedded Systems Security for Windows

Caso tenha incluído o componente 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 for Windows usando o Simple Network Management Protocol (SNMP).

Para exibir os Medidores e as interceptações do Kaspersky Embedded Systems Security for Windows na estação de trabalho do administrador, inicie o Serviço SNMP no dispositivo protegido e os Serviços SNMP e de Interceptação SNMP na estação de trabalho do administrador.

Contadores SNMP do Kaspersky Embedded Systems Security for Windows

Esta seção contém tabelas com uma descrição das configurações para os contadores SNMP do Kaspersky Embedded Systems Security for Windows.

Contadores de desempenho

Contadores de desempenho

Contador	Definição

currentRequestsAmount	Número de solicitações enviadas para serem processadas
currentInfectedQueueLength	Número de elementos na fila de objetos infectados
currentObjectProcessingRate	Número de objetos processados por segundo
currentWorkProcessesNumber	Número atual de processos de trabalho usados pelo Kaspersky Embedded Systems Security for Windows

Contadores de Quarentena

Contadores de Quarentena

Contador	Definição
totalObjects	Número de objetos atualmente na Quarentena
totalSuspiciousObjects	Número de objetos possivelmente infectados atualmente na Quarentena
currentStorageSize	Quantidade total de dados na Quarentena (MB)

Contador de Backup

Contador de Backup

Contador	Definição
currentBackupStorageSize	Quantidade total de dados no Backup (MB)

Contadores gerais

Contadores gerais

Contador	Definição
lastCriticalAreasScanAge	O período desde a última verificação completa das áreas críticas do dispositivo protegido (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 e uma chave adicional tiverem sido adicionadas, a data de expiração da licença associada à chave adicional é exibida.
currentApplicationUptime	O tempo que o Kaspersky Embedded Systems Security for Windows está em execução desde que foi iniciado pela última vez, em centenas de segundos.

Contador de Atualização

Contador de Atualização

Contador	Definição
avBasesAge	"Idade" dos bancos de dados (tempo decorrido em centésimos de segundos desde a data de criação da última atualização do banco de dados instalada).

Contadores de Proteção de Arquivos em Tempo Real

Contadores de Proteção de Arquivos 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 for Windows; 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 for Windows 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
totalObjectsDisinfected	Número total de objetos infectados desinfectados pelo Kaspersky Embedded Systems Security for Windows; 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 for Windows 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 excluídos pelo Kaspersky Embedded Systems Security for Windows; 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 for Windows tentou excluir, 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 for Windows; 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 for Windows 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 do SNMP no Kaspersky Embedded Systems Security for Windows e suas opções

As opções de interceptações do SNMP no Kaspersky Embedded Systems Security for Windows são resumidas como os seguintes:

- eventThreatDetected: um objeto foi detectado.

  A interceptação tem as seguintes opções:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds: tamanho máximo do Backup excedido. O tamanho total dos dados do Backup excedeu o valor especificado pelo **Tamanho máximo do backup (MB)**. O Kaspersky Embedded Systems Security for Windows continua a fazer backup de objetos infectados.

  A interceptação tem as seguintes opções:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds: limite de espaço disponível no backup atingido. O volume de espaço disponível no Backup é menor ou igual ao valor especificado pelo **Valor limite de espaço disponível (MB)**. O Kaspersky Embedded Systems Security for Windows continua a fazer backup de objetos infectados.

  A interceptação tem as seguintes opções:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventQuarantineStorageSizeExceeds: tamanho máximo da Quarentena excedido. O tamanho total dos dados da Quarentena excedeu o valor especificado pelo **Tamanho máximo da Quarentena (MB)**. O Kaspersky Embedded Systems Security for Windows continua a colocar na Quarentena os objetos possivelmente infectados.

  A interceptação tem as seguintes opções:

- 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 igual ou inferior ao valor especificado. O Kaspersky Embedded Systems Security for Windows continua a fazer backup de objetos infectados.

  A interceptação tem as seguintes opções:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined: erro de quarentena.

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason

- eventObjectNotBackuped: Erro ao salvar uma cópia de objeto no Backup.

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason

- eventQuarantineInternalError: erro interno de Quarentena.

  A interceptação tem as seguintes opções:

- eventSeverity
- eventDateAndTime
- eventSource
- eventReason

- eventBackupInternalError: erro de Backup.

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated: o banco de dados do antivírus está desatualizado. 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 dispositivos protegidos).

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - dias

- eventAVBasesTotallyOutdated: o banco de dados do antivírus está obsoleto. 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 dispositivos protegidos).

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - dias

- eventApplicationStarted: o Kaspersky Embedded Systems Security for Windows está sendo executado.

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventApplicationShutdown: o Kaspersky Embedded Systems Security for Windows está interrompido.

A interceptação tem as seguintes opções:

- eventSeverity
- eventDateAndTime
- eventSource

- eventCriticalAreasScanWasntPerformForALongTime: as áreas críticas não são verificadas há muito tempo. Número de dias desde a última conclusão da tarefa de Verificação de Áreas Críticas.

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - dias

- eventLicenseHasExpired: a licença expirou.

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon: a licença expira em breve. Calculado como o número de dias até a data de expiração da licença.

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - dias

- eventTaskInternalError: erro ao concluir a tarefa.

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName

- eventUpdateError: Erro ao executar a tarefa de atualização.

  A interceptação tem as seguintes opções:

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

O SNMP do Kaspersky Embedded Systems Security for Windows intercepta descrições de opções e valores possíveis

As descrições das opções de interceptação e seus possíveis valores são dadas abaixo:

- eventDateAndTime: data e hora do evento.
- eventSeverity: nível de importância.

  A opção pode ter os seguintes valores:

  - critical (1) – crítico
  - warning (2) – aviso
  - info (3) – informativo
- userName: nome de usuário (por exemplo, o nome de um usuário que tentou acessar um arquivo infectado).
- computerName: nome do dispositivo protegido (por exemplo, o nome de um dispositivo protegido a partir do qual um usuário tentou acessar um arquivo infectado).
- eventSource: componente funcional que gerou o evento.

  A opção pode ter os seguintes valores:

  - unknown (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 à operação do Kaspersky Embedded Systems Security for Windows como um todo, em vez da operação de componentes individuais

- systemAudit (8) – log de auditoria do sistema

- eventReason: acionador de evento: o que acionou o evento.

  A opção pode ter os seguintes valores:

  - reasonUnknown(0) – o motivo é desconhecido.

  - reasonInvalidSettings (1) – somente para os eventos de Backup e Quarentena. Exibido se a pasta Quarentena ou Backup estiver indisponível (permissões de acesso insuficientes ou uma pasta inválida é especificada nas configurações de Quarentena, por exemplo, um caminho de rede é especificado). Nesse caso, o Kaspersky Embedded Systems Security for Windows usará a pasta padrão do Backup ou da Quarentena.

- objectName: um nome de objeto (por exemplo, o nome do arquivo no qual o vírus foi detectado).

- threatName: o nome do objeto de acordo com a classificação da Virus Encyclopedia. Esse nome é incluído no nome completo que o Kaspersky Embedded Systems Security for Windows devolve ao detectar um objeto. Você pode exibir o nome completo de um objeto detectado no Log de tarefas.

- detectType: tipo de objeto detectado.

  A opção pode ter os seguintes valores:

  - undefined (0) – indefinido

  - virware – vírus clássicos e worms de rede

  - trojware – cavalos de Troia

  - malware – outros aplicativos maliciosos

  - adware – software de publicidade

  - pornware – software de pornografia

  - riskware: aplicativos legítimos que podem ser usados por invasores para danificar os dados pessoais ou o dispositivo do usuário

- detectCertainty: nível de certeza de detecção da ameaça.

  A opção pode ter os seguintes valores:

  - Suspeita (possivelmente infectado) – o Kaspersky Embedded Systems Security for Windows detectou uma correspondência parcial entre uma seção de código do objeto e uma seção conhecida de código malicioso.

  - Certeza (infectado) – o Kaspersky Embedded Systems Security for Windows detectou uma correspondência total entre uma seção de código no objeto e uma seção conhecida de código malicioso.

- days: número de dias (por exemplo, o número de dias até a data de expiração da licença).

- errorCode: um 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: um nome de tarefa.

- updaterErrorEventReason: o motivo do erro de atualização.

A opção pode ter os seguintes valores:

- reasonUnknown(0) – o motivo é desconhecido.
- reasonAccessDenied – acesso negado.
- reasonUrlsExhausted – a lista de fontes de atualização foi esgotada.
- 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 proxy.
- reasonServerAuthError – erro de autenticação do servidor.
- reasonHostNotFound – dispositivo não encontrado.
- reasonServerBusy – servidor indisponível.
- reasonConnectionError – erro de conexão.
- reasonModuleNotFound – objeto não encontrado.
- reasonBlstCheckFailed(16) – erro ao verificar a lista de bloqueio de chaves. É possível que estivessem sendo publicadas atualizações do banco de dados no momento da atualização; repita a atualização dentro de alguns minutos.

- storageObjectNotAddedEventReason: o motivo pelo qual o objeto não foi colocado no Backup ou Quarentena.

  A opção pode ter os seguintes valores:

  - reasonUnknown(0) – o motivo é desconhecido.
  - reasonStorageInternalError – erro de banco de dados; o Kaspersky Embedded Systems Security for Windows deve ser restaurado.
  - reasonStorageReadOnly – o banco de dados é somente-leitura; o Kaspersky Embedded Systems Security for Windows deve ser restaurado.
  - reasonStorageIOError – erro de entrada-saída: a) o Kaspersky Embedded Systems Security for Windows está corrompido e precisa ser restaurado; b) o disco onde os arquivos do Kaspersky Embedded Systems Security for Windows estão armazenados está corrompido.
  - reasonStorageCorrupted – o armazenamento está corrompido; o Kaspersky Embedded Systems Security for Windows deve ser restaurado.

- reasonStorageFull – o banco de dados está cheio; é necessário espaço livre em disco.
- reasonStorageOpenError – o arquivo de banco de dados não pode ser aberto; o Kaspersky Embedded Systems Security for Windows deve ser restaurado.
- reasonStorageOSFeatureError – alguns recursos do sistema operacional não correspondem aos requisitos do Kaspersky Embedded Systems Security for Windows.
- reasonObjectNotFound – o objeto sendo colocado na Quarentena não existe no disco.
- reasonObjectAccessError – permissões insuficientes para utilizar a API de backup: a conta sendo utilizada 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 for Windows 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 receber informações sobre o status do Kaspersky Embedded Systems Security for Windows e seus componentes.

Quando o Kaspersky Embedded Systems Security for Windows é instalado, ele registra um módulo proprietário no sistema para criar um namespace do Kaspersky Embedded Systems Security for Windows no dispositivo protegido. O namespace Kaspersky Embedded Systems Security for Windows permite trabalhar com classes e instâncias do Kaspersky Embedded Systems Security for Windows e suas propriedades.

Os valores de algumas propriedades de instâncias dependem dos tipos de tarefa.

Uma *tarefa não-periódica* é uma tarefa de aplicativo não limitada em termos de tempo e que pode estar constantemente em execução ou parada. Essas tarefas não têm progresso de execução. Os resultados da tarefa são registrados em log continuamente enquanto a tarefa é executada como eventos únicos (por exemplo, a detecção de um objeto infectado por quaisquer tarefas de Proteção do Computador em Tempo Real). Este tipo de tarefa é gerenciado por meio de políticas do Kaspersky Security Center.

Uma *tarefa periódica* é uma tarefa de aplicativo limitada em termos de tempo e cujo progresso de execução é exibido em percentuais. Os resultados da tarefa são gerados quando ela é concluída e são 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). Diversas tarefas periódicas de mesmo tipo podem ser executadas em um único dispositivo protegido simultaneamente (por exemplo, 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).

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 instalado.	Número da versão do aplicativo completo, inclusive o número da compilação.

InstalledPatches	Conjunto de nomes de exibição para patches instalados.	Lista de reparos críticos instalados para o aplicativo.
IsLicenseInstalled	Status da ativação do aplicativo.	Status da chave usada para ativar o aplicativo. Valores possíveis: • Falso - Uma chave de licença não foi adicionada no aplicativo. • Verdadeiro - Uma chave de licença foi adicionada 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 - Não é possível 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 de bloqueio de chaves).
AVBasesDatetime	Carimbo de data/hora da 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 do antivírus, o campo tem o valor "Não instalado".
IsExploitPreventionEnabled	Status 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. Caso nenhuma tarefa não periódica esteja em execução, o campo terá o valor "Nenhuma".
IsAppControlRunning	Status 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.	Descreve o 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	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.
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. Caso nenhuma instância de inicialização de aplicativo bloqueada esteja registrada no momento em que a consulta WMI for processada, o campo recebe o valor “Nenhuma”.
PeriodicTasksRunning	Conjunto de tarefas periódicas em execução no momento.	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. Caso nenhuma tarefa periódica esteja sendo executada no momento, o campo recebe o valor “Nenhuma”.
ConnectionState	Status da conexão entre o componente Provedor WMI e o Kaspersky Security Service (KAVFS).	Informações sobre o status da conexão entre o componente do Provedor de WMI e o Kaspersky Security Service. Valores possíveis: • Êxito - a conexão foi estabelecida com êxito: o cliente WMI pode receber 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 for Windows, em que:

- KasperskySecurity_ProductInfo é o nome da classe do Kaspersky Embedded Systems Security for Windows
- .ProductName=Kaspersky Embedded Systems Security for Windows são as propriedades da chave do Kaspersky Embedded Systems Security for Windows

A instância é criada no namespace ROOT\Kaspersky\Security.

Trabalhar com o Kaspersky Embedded Systems Security for Windows na linha de comando

Esta seção descreve como trabalhar com o Kaspersky Embedded Systems Security for Windows na linha de comando.

Comandos

É possível executar comandos básicos de gerenciamento do Kaspersky Embedded Systems Security for Windows a partir da linha de comando do dispositivo protegido utilizando o componente utilitário de linha de comando, incluído no grupo de componentes do software Kaspersky Embedded Systems Security for Windows.

É possível usar comandos para gerenciar apenas as funções acessíveis de acordo com as permissões atribuídas a você no Kaspersky Embedded Systems Security for Windows.

Certos comandos do Kaspersky Embedded Systems Security for Windows são realizados das seguintes maneiras:

- Modo síncrono: o controle volta ao Console somente após a conclusão do comando.
- Modo assíncrono: o controle volta ao Console imediatamente após a inicialização do comando.

Para interromper a execução de um comando no modo síncrono,

pressione o atalho **Ctrl+C** no teclado.

Siga as seguintes regras ao inserir comandos do Kaspersky Embedded Systems Security for Windows:

- Introduza modificadores e comandos usando letras maiúsculas e minúsculas.
- Separe modificadores com um espaço.
- Se o caminho de um arquivo/pasta especificado como valor incluir um espaço, coloque o caminho entre aspas, por exemplo: `"C:\TEST\test cpp.exe"`.
- Se necessário, use curingas no nome ou caminho do arquivo, por exemplo: `"C:\Temp\Temp*\"`, `"C:\Temp\Temp???.doc"`, `"C:\Temp\Temp*.doc"`.

É possível usar a linha de comando para executar todas as operações necessárias para o gerenciamento e administração do Kaspersky Embedded Systems Security for Windows (consulte a tabela abaixo).

Comandos do Kaspersky Embedded Systems Security for Windows

Comando	Descrição
KAVSHELL APPCONTROL	Atualiza a lista de regras de acordo com a regra de importação selecionada.
KAVSHELL APPCONTROL /CONFIG	Define o modo operacional da tarefa de Controle de Inicialização de Aplicativos
KAVSHELL APPCONTROL /GENERATE	Inicia a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos.

KAVSHELL VACUUM	Desfragmenta arquivos de log do Kaspersky Embedded Systems Security for Windows.
KAVSHELL PASSWORD	Gerencia as configurações de proteção de senha.
KAVSHELL HELP	Exibe a ajuda do comando para o Kaspersky Embedded Systems Security for Windows.
KAVSHELL START	Inicia o Kaspersky Security Service.
KAVSHELL STOP	Interrompe o Kaspersky Security Service.
KAVSHELL SCAN	Cria e inicia uma tarefa de Verificação por Demanda temporária com o escopo da verificação e as configurações de segurança especificadas pelas opções da linha de comando.
KAVSHELL SCANCRITICAL	Inicia uma tarefa local do sistema de Verificação de áreas críticas.
KAVSHELL TASK	Inicia, pausa, retoma ou para a tarefa especificada de forma assíncrona. Retorna o status atual da tarefa/estatísticas da tarefa.
KAVSHELL RTP	Inicia ou interrompe todas as tarefas de Proteção do Computador em Tempo Real.
KAVSHELL UPDATE	Inicia a tarefa de Atualização do Banco de Dados com as configurações especificadas pelas opções de linha de comando.
KAVSHELL ROLLBACK	Reverte os bancos de dados para a versão anterior.
KAVSHELL LICENSE	Adiciona ou elimina as chaves. Exibe informações sobre as chaves adicionadas.
KAVSHELL TRACE	Ativa ou desativa o rastreamento. Gerencia as configurações de rastreamento.
KAVSHELL DUMP	Ativa ou desativa a criação de arquivos de despejo em caso de encerramento anormal de processos do Kaspersky Embedded Systems Security for Windows.
KAVSHELL IMPORT	Importa configurações gerais, funções e tarefas do Kaspersky Embedded Systems Security for Windows de um arquivo de configuração.
KAVSHELL EXPORT	Exporta todas as configurações e tarefas existentes do Kaspersky Embedded Systems Security for Windows para um arquivo de configuração.
KAVSHELL DEVCONTROL	Adiciona à lista de regras de controle de dispositivos gerada de acordo com o método selecionado.

Exibição do comando de ajuda do Kaspersky Embedded Systems Security for Windows. KAVSHELL HELP

Para visualizar a lista de todos os comandos do Kaspersky Embedded Systems Security for Windows, execute um dos comandos a seguir:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Para visualizar uma descrição de um comando e sua sintaxe, execute um dos comandos a seguir:

```
KAVSHELL HELP <comando>

KAVSHELL <comando> /?
```

Exemplos de KAVSHELL HELP

Para exibir informações detalhadas sobre o comando KAVSHELL SCAN, execute o seguinte comando:

```
KAVSHELL HELP SCAN
```

Inicialização e interrupção do Kaspersky Security Service: KAVSHELL START, KAVSHELL STOP

Para rodar o Kaspersky Security Service, execute o seguinte 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 Operacional, bem como outras tarefas programadas para iniciar **Ao iniciar o aplicativo**, serão iniciadas.

Para interromper o Kaspersky Security Service, execute o seguinte comando:

```
KAVSHELL STOP
```

Uma senha pode ser necessária para executar o comando. Para digitar a senha atual, use `[/pwd:<senha>]`.

Verificação de um escopo especificado: KAVSHELL SCAN

Para iniciar uma tarefa para verificar áreas específicas do dispositivo protegido, use `KAVSHELL SCAN`. As opções da linha de comando especificam o escopo da verificação e as configurações de segurança do node selecionado.

Uma 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). Contudo, um log de tarefas é gerado e exibido nos **Logs de tarefas** no Console do Aplicativo.

Ao especificar caminhos em tarefas de verificação para áreas específicas, é possível pode usar variáveis de ambiente. Caso use a variável de ambiente, execute o comando `KAVSHELL SCAN` como o usuário correspondente.

O comando `KAVSHELL SCAN` é executado no modo síncrono.

Para iniciar uma tarefa de Verificação por Demanda existente na linha de comando, use o comando KAVSHELL TASK.

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 de 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 do arquivo de log de tarefas>]
[/ANSI] [/ALIAS:<alias da tarefa>]
```

O comando KAVSHELL SCAN tem parâmetros/opções obrigatórios e opcionais (veja a tabela abaixo).

Exemplo do comando KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\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
```

Parâmetros/opções da linha de comando KAVSHELL SCAN

Parâmetro/opção	Descrição
Escopo da verificação. A configuração é obrigatória.	
<arquivos>	Especifica o escopo da verificação - lista de arquivos, pastas, caminhos de rede e áreas predefinidas. Especifique caminhos de rede no formato UNC (Universal Naming Convention). No exemplo a seguir, Folder4 é especificado sem o caminho para ele. Isso significa que ele está localizado na pasta a partir da qual o comando KAVSHELL é executado. KAVSHELL SCAN Pasta4 Se o nome do objeto a ser verificado tiver espaços, ele deverá ser colocado entre aspas. Se uma pasta for especificada, o Kaspersky Embedded Systems Security for Windows também verificará todas as suas subpastas. Os símbolos * ou ? podem ser usados para verificar um grupo de arquivos.
<pastas>	
<caminho de rede>	
/MEMORY	Verificar objetos da RAM
/SHARED	Verificar pastas compartilhadas do dispositivo protegido
/STARTUP	Verificar objetos de execução automática
/REMDRIVES	Verificar unidades removíveis
/FIXDRIVES	Verificar discos rígidos
/MYCOMP	Verificar todas as áreas do dispositivo protegido
/L:<caminho do arquivo com uma	Caminho completo do arquivo com uma lista de escopos da verificação.

lista de escopos da verificação>	Use quebras de linha para separar os escopos da verificação no arquivo. É possível especificar áreas de verificação predefinidas, como mostrado no seguinte exemplo do conteúdo de um arquivo com uma lista de escopos da verificação: C:\ D:\Docs*.doc E:\Meus Documentos /STARTUP /SHARED
Verificar objetos (Tipos de arquivo). Caso você não especifique essa opção, o Kaspersky Embedded Systems Security for Windows vai verificar objetos pelo seu formato.	
/FA	Verificar todos os objetos
/FC	Verificar objetos por formato (padrão). O Kaspersky Embedded Systems Security for Windows verifica somente objetos cujo formato estão incluídos na lista de formatos de objetos infectáveis.
/FE	Verificar objetos por extensão. O Kaspersky Embedded Systems Security for Windows verifica somente objetos com extensões incluídas na lista de extensões de objetos infetáveis.
/NEWONLY	Verificar apenas arquivos novos e modificados. Caso você não forneça essa opção, o Kaspersky Embedded Systems Security for Windows vai verificar todos os objetos.
Ação a ser executada em objetos infectados e outros. Se você não especificar valores para esse modificador, o Kaspersky Embedded Systems Security for Windows executará a ação **Ignorar**.	
DISINFECT	Desinfectar; ignorar se a desinfecção não for possível As opções DISINFECT e DELETE foram preservadas na versão atual do Kaspersky Embedded Systems Security for Windows para garantir a compatibilidade com versões anteriores. Essas opções podem ser usadas no lugar das opções /AI e /AS. Nesse caso, o Kaspersky Embedded Systems Security for Windows não processará os objetos possivelmente infectados.
DISINFDEL	Desinfectar; excluir se a desinfecção não for possível
DELETE	Excluir As opções DISINFECT e DELETE foram preservadas na versão atual do Kaspersky Embedded Systems Security for Windows para garantir a compatibilidade com versões anteriores. Essas opções podem ser usadas no lugar das opções /AI e /AS. Nesse caso, o Kaspersky Embedded Systems Security for Windows não processará os objetos possivelmente infectados.
REPORT	Enviar relatório (padrão)
AUTO	Executar ação recomendada
Ação a ser executada em objetos possivelmente infectados. Caso você não especifique essa opção, o Kaspersky Embedded Systems Security for Windows executará a ação **Ignorar**.	
QUARANTINE	Quarentena
DELETE	Excluir
REPORT	Enviar relatório (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"`.
/ET:<número de segundos>	Interrompe o processamento de um objeto se ele ultrapassar o número de segundos especificado pelo <número de segundos>. Por padrão, não há 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 for Windows 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: <nível de análise heurística>	Ativa o Analisador Heurístico, configura o nível de análise. Estão disponíveis os seguintes níveis de análise heurística: 1 – superficial 2 – médio 3 – profundo Caso você omita essa opção, o Kaspersky Embedded Systems Security for Windows não usará o Analisador heurístico.
/ALIAS:<alias da tarefa>	Atribui um nome temporário a uma tarefa de Verificação por Demanda, permitindo consultá-la durante a execução, por exemplo, para visualizar suas estatísticas usando o comando TASK. O alias da tarefa deve ser exclusivo entre os aliases de tarefas de todos os componentes do Kaspersky Embedded Systems Security for Windows. Se essa opção não for especificada, é atribuído um nome temporário no formato scan_<kavshell_pid>; por exemplo, scan_1234. No Console do Aplicativo, a tarefa recebe o nome "Verificar objetos <dia e hora>", por exemplo, Verificar objetos 16/08/2007 17h13m14.
Configurações do log de tarefas (Configurações de relatórios)	
/W:<caminho do arquivo de log de tarefas>	Se esse parâmetro for especificado, o Kaspersky Embedded Systems Security for Windows salvará o arquivo de log de tarefas usando o nome especificado pelo valor do parâmetro. O arquivo de log contém estatísticas de execução da tarefa, a hora em que ela foi iniciada e concluída (interrompida), além de informações sobre eventos ocorridos durante a tarefa. O log é usado para registrar eventos definidos pelas configurações do log de tarefas e do log de eventos do Kaspersky Embedded Systems Security for Windows no Visualizador de Eventos.

	É possível especificar o caminho absoluto ou relativo do arquivo de log. Se você especificar somente um nome de arquivo sem um 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 node Logs de tarefas do Console do Aplicativo. Se o Kaspersky Embedded Systems Security for Windows não conseguir criar o arquivo de log, ele exibirá uma mensagem de erro, mas ainda executará o comando.
/ANSI	Essa opção usa a codificação ANSI para registrar eventos no log de tarefas. A opção ANSI não será aplicada se o parâmetro W não for especificado. Se a opção ANSI não for especificada, o log de tarefas é gerado usando o UNICODE.

Iniciando a tarefa de Verificação de áreas críticas: KAVSHELL SCANCRITICAL

Use o comando `KAVSHELL SCANCRITICAL` para iniciar a tarefa de 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 de Áreas Críticas e salvar o log de tarefas scancritical.log na pasta atual, execute o seguinte comando:

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

É possível usar o parâmetro /W para configurar a localização do log de tarefas (consulte a tabela abaixo).

Sintaxe do parâmetro `/W` para o comando `KAVSHELL SCANCRITICAL`

Parâmetro/opção	Descrição
/W:<caminho do arquivo de log de tarefas>	Se esse parâmetro for especificado, o Kaspersky Embedded Systems Security for Windows salvará o arquivo de log de tarefas usando o nome especificado pelo valor do parâmetro. O arquivo de log contém estatísticas de execução da tarefa, a hora em que ela foi iniciada e concluída (interrompida), além de informações sobre eventos ocorridos durante a tarefa. O log é usado para registrar eventos definidos pelas configurações do log de tarefas e do log de eventos do Kaspersky Embedded Systems Security for Windows no Visualizador de Eventos. É possível especificar o caminho absoluto ou relativo do arquivo de log. Se você especificar somente um nome de arquivo sem um 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 node **Logs de tarefas** do Console do Aplicativo. Se o Kaspersky Embedded Systems Security for Windows não conseguir criar o arquivo de log, ele exibirá uma mensagem de erro, mas ainda executará o comando.

Gerenciando tarefas de forma assíncrona: KAVSHELL TASK

É possível usar o comando `KAVSHELL TASK` para gerenciar a tarefa especificada: executar, pausar, continuar e interromper a tarefa e visualizar o status e as estatísticas atuais da tarefa. Este comando é executado no modo assíncrono.

Uma senha pode ser necessária para executar o comando. Para digitar a senha atual, use `[/pwd:<senha>]`.

Sintaxe do comando KAVSHELL TASK

```
KAVSHELL TASK [<alias do nome da tarefa> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Exemplo do comando KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE

KAVSHELL TASK network-attack-blocker /START
```

O comando `KAVSHELL TASK` pode ser executado sem parâmetros/opções ou com um ou mais parâmetros/opções (consulte a tabela abaixo).

Parâmetros/opções da linha de comando KAVSHELL TASK

Parâmetro/opção	Descrição
Nenhum parâmetro	Mostra a lista de todas as tarefas existentes do Kaspersky Embedded Systems Security for Windows. A lista contém os seguintes campos: alias da tarefa, categoria da tarefa (de 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 for Windows às tarefas. Para visualizar os aliases de tarefa do Kaspersky Embedded Systems Security for Windows, insira o comando KAVSHELL TASK sem nenhum parâmetro.
/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	Retornar ao status atual da tarefa (por exemplo, *Executando*, *Concluída*, *Pausada*, *Interrompida*, *Falhou*, *Iniciando*, *Reiniciando*)
/STATISTICS	Obter estatísticas da tarefa - informações sobre o número de objetos processados a partir da hora de início da tarefa

Observe que nem todas as tarefas do Kaspersky Embedded Systems Security for Windows são totalmente compatíveis com as chaves /PAUSE, /RESUME e /STATE.

Códigos de retorno do comando KAVSHELL TASK.

Remoção do atributo PPL: KAVSHELL CONFIG

O comando `KAVSHELL CONFIG` permite remover o atributo PPL (Protected Process Light, Processo protegido superficial) do Kaspersky Security Service usando o driver ELAM instalado durante a instalação do aplicativo.

Sintaxe do comando KAVSHELL CONFIG

```
KAVSHELL CONFIG /PPL:<OFF>
```

Parâmetros/opções da linha de comando KAVSHELL CONFIG

Parâmetro/opção	Descrição
/PPL:OFF	Remover o atributo de PPL para o Kaspersky Security Service.

Inicialização e interrupção de tarefas de Proteção do Computador em Tempo Real. KAVSHELL RTP

É possível usar o comando `KAVSHELL RTP` para iniciar ou interromper todas as tarefas de Proteção do Computador em Tempo Real.

Uma senha pode ser necessária para executar o comando. Para digitar a senha atual, use `[/pwd:<senha>]`.

Sintaxe do comando KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Exemplo do comando KAVSHELL RTP

Para executar todas as tarefas de Proteção do Computador em Tempo Real, execute o seguinte comando:

```
KAVSHELL RTP /START
```

O comando `KAVSHELL RTP` deve incluir uma das duas opções (consulte a tabela abaixo).

Opções da linha de comando KAVSHELL RTP

Parâmetro/opção	Descrição
/START	Inicia todas as tarefas de Proteção do Computador em Tempo Real: Proteção de Arquivos em Tempo Real e Uso da KSN.
/STOP	Interromper todas as tarefas de Proteção do Computador 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 monitorar o carregamento de 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).

Parâmetros/opções da linha de comando `KAVSHELL APPCONTROL /CONFIG`

Parâmetro/opção	Descrição
`/mode:<applyrules|statistics>`	Modo da tarefa de Controle de Inicialização de Aplicativos. Você pode selecionar um dos seguintes modos: • ativa - aplicar regras de Controle de Inicialização de Aplicativos; • statistics - somente gera estatísticas.
`/dll:<no|yes>`	Ativa ou desativa o monitoramento do carregamento de DLL.
`/savetofile: <caminho completo para o arquivo XML>`	Exportar as regras especificadas para o arquivo indicado no formato XML.
`/savetofile: <nome completo para o arquivo XML>`	Salvar a lista de regras no arquivo.

`/savetofile: <nome completo para o arquivo XML> /sdc`	Salvar a lista de regras de Controle de Distribuição de Software no arquivo.
`/clearsdc`	Excluir todas as regras de Controle de Distribuição de Software da lista.

Gerador de Regras de Controle de Inicialização de Aplicativos: KAVSHELL APPCONTROL /GENERATE

É possível usar o comando `KAVSHELL APPCONTROL /GENERATE` para gerar listas de regras de Controle de Inicialização de Aplicativos.

Uma senha pode ser necessária para executar o comando. Para digitar a senha atual, use `[/pwd:<senha>]`.

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 com qualquer extensão na pasta especificada e, após a conclusão da 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
```

É possível usar os parâmetro/opções da linha de comando para definir as configurações de geração automática de regras para a tarefa de Controle de Inicialização de Aplicativos (consulte a tabela abaixo).

Parâmetros/opções da linha de comando `KAVSHELL APPCONTROL /GENERATE`

Parâmetro/opção	Descrição
Escopo de uso das regras de permissão	
<caminho da pasta>	Especifique o caminho para a pasta com arquivos executáveis para os quais as regras de permissão serão geradas automaticamente.
/source: <caminho para o arquivo com lista de pastas>	Especifique o caminho para um arquivo TXT com uma lista de pastas com arquivos executáveis para os quais as regras de permissão serão geradas automaticamente.
/ máscaras:	Especifique as extensões de arquivos executáveis para os quais as regras de permissão

<edms>	serão geradas automaticamente. É possível incluir arquivos com as seguintes extensões no escopo das regras: • e - Arquivos EXE • d - Arquivos DLL • m - Arquivos MSI • s - scripts
/runapp	Ao gerar regras de permissão, considere aplicativos em execução no dispositivo protegido no momento.
Ações ao gerar regras de permissão automaticamente	
/rules: <ch|cp|h>	Especifique ações a serem executadas ao gerar regras de permissão para a tarefa de Controle de Inicialização de Aplicativos: • ch - Usar o certificado digital. Se o certificado estiver ausente, use o hash SHA256. • cp - Usar o certificado digital. Se o certificado estiver ausente, use o caminho do arquivo executável. • h - Usar o hash SHA256.
/strong	Usar o requerente e a impressão digital do certificado digital ao gerar automaticamente regras de permissão para a tarefa de Controle de Inicialização de Aplicativos. O comando é executado caso um valor seja especificado para a opção /rules: <ch|cp>.
/user: <usuário ou grupo de usuários>	Especifica o usuário ou grupo de usuários para os quais as regras serão aplicadas. O aplicativo controlará qualquer aplicativo executado pelo usuário e/ou grupo de usuários especificado.
Ações na conclusão da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos	
/export: <caminho completo para o arquivo XML>	Salva as regras geradas em um arquivo XML.
/unique	Adiciona informações sobre o dispositivo protegido com aplicativos instalados que são a base para a geração de regras de permissão de Controle de Inicialização de Aplicativos.
/prefix: <prefixo para nomes de regras>	Especifica um prefixo para o nome de regras de permissão de Controle de Inicialização de Aplicativos.
/import: <a|r|m>	Importa as regras geradas para a lista de regras de controle de inicialização de aplicativos especificada de acordo com a regra de importação selecionada: • a - **Adicionar às regras existentes** (regras com configurações idênticas são duplicadas) • r - **Substituir as regras existentes** (regras com configurações idênticas não são adicionadas; uma regra é adicionada se pelo menos uma configuração de regra for única) • r - **Mesclar com as regras existentes** (regras com configurações idênticas não são adicionadas; uma regra é adicionada se pelo menos uma configuração de regra for

	única)

Preenchimento da lista de regras de Controle de Inicialização de Aplicativos. KAVSHELL APPCONTROL

É possível usar o comando `KAVSHELL APPCONTROL` para adicionar as regras de um arquivo XML à lista de regras da tarefa de Controle de Inicialização de Aplicativos de acordo com a regra de importação selecionada, além de excluir todas as regras existentes da lista.

Uma senha pode ser necessária para executar o comando. Para digitar a senha atual, use `[/pwd:<senha>]`.

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 a regras de Controle de Inicialização de Aplicativos existentes de acordo com a regra de importação Adicionar às regras existentes, execute o seguinte comando:

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

É possível usar as opções da linha de comando para selecionar o princípio de adição de novas regras do arquivo XML especificado na lista definida de regras de Controle de Inicialização de Aplicativos (consulte a tabela abaixo).

Parâmetros/opções da linha de comando `KAVSHELL APPCONTROL`

Parâmetro/opção	Descrição
/append <caminho para arquivo XML>	Atualiza a lista de regras de controle de inicialização de aplicativos com base no arquivo XML especificado. Regra de importação - **Adicionar às regras existentes**(regras com configurações idênticas são duplicadas).
/replace <caminho para arquivo XML>	Atualiza a lista de regras de controle de inicialização de aplicativos com base no arquivo XML especificado. Regra de importação - **Substituir as regras existentes** (regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos uma configuração de regra for única).
/merge <caminho para arquivo XML>	Atualiza a lista de regras de controle de inicialização de aplicativos com base no arquivo XML especificado. Regra de importação - **Mesclar com as regras existentes** (novas regras não duplicam regras já existentes).
/clear	Apagar a lista de regras de Controle de Inicialização de Aplicativos.

Preenchimento da lista de regras de Controle de Dispositivos. KAVSHELL DEVCONTROL

É possível usar o comando `KAVSHELL DEVCONTROL` para adicionar regras de um arquivo XML à lista de regras da tarefa de Controle de Dispositivos de acordo com a regra de importação selecionada, além de excluir todas as regras existentes da lista.

Uma senha pode ser necessária para executar o comando. Para digitar a senha atual, use `[/pwd:<senha>]`.

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 as regras de um arquivo XML às regras de controle de dispositivos existentes de acordo com a regra de importação Adicionar às regras existentes, execute o seguinte comando:

```
KAVSHELL DEVCONTROL /append c:\rules\devctrlrules.xml
```

É possível usar as opções da linha de comando para selecionar a regra de importação usada para adicionar novas regras do arquivo XML especificado à lista definida de regras de Controle de Dispositivos (consulte a tabela abaixo).

Parâmetros/opções da linha de comando `KAVSHELL DEVCONTROL`

Chave	Descrição
/append <caminho para arquivo XML>	Atualiza a lista de regras de Controle de Dispositivos com base no arquivo XML especificado. Regra de importação - **Adicionar às regras existentes**(regras com configurações idênticas são duplicadas).
/replace <caminho para arquivo XML>	Atualiza a lista de regras de Controle de Dispositivos com base no arquivo XML especificado. Regra de importação - **Substituir as regras existentes** (regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos uma configuração de regra for única).
/merge <caminho para arquivo XML>	Atualiza a lista de regras de Controle de Dispositivos com base no arquivo XML especificado. Regra de importação - **Mesclar com as regras existentes** (novas regras não duplicam regras já existentes).
/clear	Apaga a lista de regras de Controle de Dispositivos.

Inicialização da tarefa de Atualização do Banco de Dados: KAVSHELL UPDATE

O comando `KAVSHELL UPDATE` pode ser usado para iniciar tarefa de atualização do banco de dados do Kaspersky Embedded Systems Security for Windows em modo assíncrono.

Uma tarefa de Atualização do banco de dados iniciada usando o comando `KAVSHELL UPDATE` é uma tarefa temporária. Ela é exibida apenas no Console do Aplicativo ao ser executada. Contudo, um log de tarefas é gerado e exibido nos **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 a utilização do Kaspersky Security Center para gerenciar o Kaspersky Embedded Systems Security for Windows em dispositivos protegidos, consulte a seção "Gerenciamento do Kaspersky Embedded Systems Security for Windows por meio do Kaspersky Security Center".

É possível usar variáveis de ambiente ao especificar o caminho de uma fonte de atualização nesta tarefa. Se uma variável de ambiente do usuário for usada, execute o comando `KAVSHELL UPDATE` como o usuário correspondente.

Sintaxe do comando KAVSHELL UPDATE

```
KAVSHELL UPDATE < Caminho para atualizar a fonte | /AK | /KL> [/NOUSEKL] [/PROXY:
<endereço>:<porta>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nome de usuário>] [/PROXYPWD:<senha>]
[/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE] [/REG:<código iso3166>] [/W:<caminho
para o arquivo de log da tarefa>] [/ALIAS:<alias da tarefa>]
```

O comando KAVSHELL UPDATE tem parâmetros/opções obrigatórios e opcionais (veja a tabela abaixo).

Exemplos do comando KAVSHELL UPDATE

Para iniciar uma tarefa de Atualização do banco de dados personalizada, execute o seguinte comando:

```
KAVSHELL UPDATE
```

Para executar a tarefa de Atualização do banco de dados usando arquivos de atualização na pasta de rede \\server\databases, execute o seguinte comando:

```
KAVSHELL UPDATE \\server\databases
```

Para iniciar uma Atualização do Banco de Dados no servidor FTP ftp://dnl-ru1.kaspersky-labs.com/ e registrar todos os eventos da tarefa em um arquivo com nome c:\update_report.log, execute o seguinte 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 for Windows do servidor de atualização da Kaspersky, conecte-se à fonte de atualizações por meio de um servidor proxy (endereço do servidor proxy: proxy.company.com, porta: 8080). Para acessar o dispositivo protegido usando a autenticação NTLM integrada do Microsoft Windows com o nome de usuário "inetuser" e senha "123456", execute o seguinte comando:

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

Parâmetros/opções da linha de comando KAVSHELL UPDATE

Parâmetro/opção	Descrição
Fonte de atualização (parâmetro obrigatório). Especifique uma ou mais fontes. O Kaspersky Embedded Systems Security for Windows acessará as fontes na ordem em que elas forem listadas. Separe as fontes 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 atualização definida pelo usuário. Endereço do servidor HTTP ou FTP onde a pasta de atualização está localizada.
<Pasta local>	Fonte de atualização definida pelo usuário. Pasta no dispositivo protegido.
/AK	Use o Servidor de Administração do Kaspersky Security Center como a fonte de atualizações.
/KL	Use os servidores de atualização da Kaspersky como fonte de atualizações.
/NOUSEKL	Não use os servidores de atualização da Kaspersky se não houver outras fontes de atualização disponíveis (usadas por padrão).
Configurações do servidor proxy	
/PROXY:<endereço>:<porta>	Nome de rede ou endereço IP do servidor proxy e sua porta. Se esse parâmetro não for especificado, o Kaspersky Embedded Systems Security for Windows detectará automaticamente as configurações do servidor proxy usado na rede local.
/AUTHTYPE:<0-2>	Esse parâmetro especifica o método de autenticação usado para acessar o servidor proxy. Ele pode ter os seguintes valores: **0** – autenticação NTLM do Microsoft Windows; o Kaspersky Embedded Systems Security for Windows fará contato com o servidor proxy usando a conta **Sistema local** (**SYSTEM**) **1** – autenticação NTLM do Microsoft Windows; o Kaspersky Embedded Systems Security for Windows fará contato com o servidor proxy usando o nome de usuário e a senha especificados pelos parâmetros /PROXYUSER e /PROXYPWD **2** – autenticação usando o nome de usuário e senha especificados pelos parâmetros /PROXYUSER e /PROXYPWD (autenticação básica) Se o servidor proxy não exigir autenticação, não é necessário especificar esse parâmetro.
/PROXYUSER:<nome de usuário>	Nome de usuário que será usado para acessar o servidor proxy. Se /AUTHTYPE:0 for especificado, os parâmetros /PROXYUSER:<nome de usuário> e /PROXYPWD:<senha> serão ignorados.
/PROXYPWD:<senha>	A senha de usuário que será usada para acessar o servidor proxy. Se /AUTHTYPE:0 for especificado, os parâmetros /PROXYUSER:<nome de usuário> e /PROXYPWD:<senha> serão ignorados. Se o parâmetro /PROXYUSER for especificado e o parâmetro /PROXYPWD for omitido, a senha será considerada como uma cadeia de caracteres vazia.
/NOPROXYFORKL	Não usar as configurações do servidor proxy para se conectar aos servidores de atualização da Kaspersky (usadas por padrão).
/USEPROXYFORCUSTOM	Usar as configurações do servidor proxy para se conectar às fontes de atualização 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, a configuração **Ignorar servidor proxy para endereços locais** será aplicada.
Configurações gerais do servidor FTP e HTTP	
/NOFTPPASSIVE	Se essa chave for especificada, o Kaspersky Embedded Systems Security for Windows usará o modo de servidor FTP ativo para se conectar ao dispositivo protegido. Se esta chave não for especificada, o Kaspersky Embedded

	Systems Security for Windows 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 esse parâmetro, o Kaspersky Embedded Systems Security for Windows usará o valor padrão de 10 segundos. O valor do parâmetro deve ser um número inteiro.
/REG:<código iso3166>	Configurações regionais. Esse parâmetro é usado ao receber atualizações de servidores de atualização da Kaspersky. O Kaspersky Embedded Systems Security for Windows minimiza a carga no dispositivo protegido por meio da seleção do servidor de atualização mais próximo. O valor desse parâmetro deve ser o código ISO 3166-1 alpha-2 do país onde o dispositivo protegido está localizado; por exemplo, /REG: gr ou /REG:US. Caso esta opção seja omitida ou um código de país inválido seja especificado, o Kaspersky Embedded Systems Security for Windows detectará a localização do dispositivo protegido de acordo com as configurações regionais do dispositivo protegido onde o Console do Aplicativo estiver instalado.
/ALIAS:<alias da tarefa>	Esse parâmetro possibilita atribuir um nome temporário à tarefa, permitindo consultar a tarefa enquanto ela é executada. 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 do Kaspersky Embedded Systems Security for Windows. Se essa chave não for especificada, é usado um nome temporário no formato update_<kavshell_pid>; por exemplo, update_1234. No Console do Aplicativo, é atribuído à tarefa o nome "Atualização do Banco de Dados <data hora>"; por exemplo, Atualização do Banco de Dados 16/08/2007 17h41m02.
/W:<caminho do arquivo de log de tarefas>	Se esse parâmetro for especificado, o Kaspersky Embedded Systems Security for Windows salvará o arquivo de log de tarefas usando o nome especificado pelo valor do parâmetro. O arquivo de log contém estatísticas de execução da tarefa, a hora em que ela foi iniciada e concluída (interrompida), além de informações sobre eventos ocorridos durante a tarefa. O log é usado para registrar eventos definidos pelas configurações do log de tarefas e do log de eventos do Kaspersky Embedded Systems Security for Windows no Visualizador de Eventos. É possível especificar o caminho absoluto ou relativo do arquivo de log. Se você especificar somente um nome de arquivo sem um 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 node **Logs de tarefas** do Console do Aplicativo. Se o Kaspersky Embedded Systems Security for Windows não conseguir criar o arquivo de log, ele exibirá uma mensagem de erro, mas ainda executará o comando.

Códigos de retorno do comando KAVSHELL UPDATE.

Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security for Windows: KAVSHELL ROLLBACK

O comando `KAVSHELL ROLLBACK` pode ser usado para executar uma tarefa local do sistema de Reversão da Atualização do Banco de Dados (reverte os bancos de dados do Kaspersky Embedded Systems Security for Windows para a versão instalada anteriormente). O comando é executado de forma síncrona.

Sintaxe do comando

```
KAVSHELL ROLLBACK
```

Códigos de retorno do comando KAVSHELL ROLLBACK.

Gerenciamento da Inspeção do Log: KAVSHELL TASK LOG-INSPECTOR

O comando `KAVSHELL TASK LOG-INSPECTOR` pode ser usado para monitorar a integridade do ambiente de acordo com uma inspeção do Log de Eventos do Windows.

Sintaxe do comando

```
KAVSHELL TASK LOG-INSPECTOR
```

Exemplos do comando

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Opções/parâmetros da linha de comando KAVSHELL TASK LOG-INSPECTOR

Parâmetro/opção	Descrição
/START	Inicia a tarefa especificada no modo assíncrono.
/STOP	Interrompe a tarefa especificada.
/STATE	Retornar ao status atual da tarefa (por exemplo, *Executando*, *Concluída*, *Pausada*, *Interrompida*, *Falhou*, *Iniciando*, *Reiniciando*)
/STATISTICS	Obter estatísticas da tarefa - informações sobre o número de objetos processados a partir da hora de início da tarefa.

Códigos de retorno do comando KAVSHELL TASK LOG-INSPECTOR.

Ativação do aplicativo. KAVSHELL LICENSE

As chaves e códigos de ativação do Kaspersky Embedded Systems Security for Windows podem ser gerenciados por meio do comando `KAVSHELL LICENSE`.

Uma senha pode ser necessária para executar o comando. Para digitar a senha atual, use `[/pwd:<senha>]`.

Sintaxe do comando KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<arquivo de chave | código de ativação> [/R] | /DEL:<chave |
número do código de ativação>]
```

Exemplos do comando KAVSHELL LICENSE

Para ativar o aplicativo, execute o comando:

```
KAVSHELL.EXE LICENSE /ADD: <código de ativação ou chave>
```

Para visualizar as informações sobre as 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 (consulte a tabela abaixo).

Parâmetros/opções da linha de comando do KAVSHELL LICENSE

Configuração	Descrição
Sem chaves	O comando retorna as seguintes informações sobre as chaves adicionadas: • Chave. • Tipo de licença (comercial). • Duração da licença associada à chave. • Status da chave (ativa ou adicional). Caso o status seja *, a chave foi adicionada como uma chave adicional.
/ADD:<nome do arquivo de chave ou código de ativação>	Adicione uma chave por meio do arquivo especificado ou um código de ativação. As variáveis do ambiente do sistema podem ser utilizadas ao especificar o caminho de um arquivo de chave; não são permitidas variáveis do ambiente do usuário.
/R	O código de ativação ou chave /R é adicional ao código ou chave de ativação /ADD e indica que o código de ativação ou chave adicionado é adicional.
/DEL:<chave ou código de ativação>	Exclui a chave com o número ou código de ativação especificado.

Códigos de retorno do comando KAVSHELL LICENSE.

Ativação, configuração e desativação de logs 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 for Windows e para configurar o nível de detalhe do log.

O Kaspersky Embedded Systems Security for Windows grava as informações nos arquivos de rastreamento e no arquivo de despejo no formulário não criptografado.

Sintaxe do comando KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:< caminho para a pasta com os arquivos de rastreamento > [/S:< tamanho máximo do arquivo de log em megabytes >] [/LVL: debug|info|warning|error|critical] [/r: < número máximo de arquivos de rastreamento para girar >] | /OFF>
```

Caso o log de rastreamento seja ativado e você desejar alterar as configurações, insira o comando `KAVSHELL TRACE` com a opção /ON e utilize os parâmetros /S e /LVL para especificar as configurações do log de rastreamento (veja a tabela abaixo).

Chaves do comando KAVSHELL TRACE

Chave	Descrição
`/ON`	Ativa o log de rastreamento.
`/F:< pasta com os arquivos de rastreamento >`	Esse parâmetro chave especifica o caminho completo da pasta em que 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. Caminhos para pastas em unidades de rede de outros dispositivos protegidos não podem ser especificados. Se o caminho especificado pelo parâmetro tiver um espaço, precisa ser colocado entre aspas, por exemplo: /F:"C:\Pasta de Rastreamento". 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 tamanho máximo, o Kaspersky Embedded Systems Security for Windows começará a gravar informações em um novo arquivo; o arquivo de log anterior será salvo. Se o valor desse parâmetro não for especificado, o tamanho máximo de um arquivo de log será 50 MB.
`/LVL:debug|info|warning|error|critical`	Esse parâmetro 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 esse parâmetro não for especificado, todos os eventos incluídos no nível de detalhamento **Todas as informações da depuração** serão registrados no log de rastreamento.
`/r:< número máximo de arquivos de rastreamento para rotação >`	Essa opção ativa a rotação dos arquivos de rastreamento. Caso a rotação do arquivo de

	rastreamento esteja ativada e o `<número máximo de arquivos de rastreamento a serem girados>` tenha sido atingido, o arquivo mais antigo será excluído antes da criação de um novo arquivo. Valores disponíveis: de 1 a 999. Caso nenhum valor seja especificado, a rotação dos arquivos de rastreamento não será ativada e o aplicativo retornará um erro.
/OFF	Esta opção desativa o log de rastreamento.

Exemplo do comando KAVSHELL TRACE

*Para ativar o log de rastreamento usando o nível de detalhamento **Todas as informações da depuração** e um tamanho máximo de log de 200 MB, salvando 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**, salvando o arquivo de log na pasta "C:\Pasta de Rastreamento", execute o comando:*

```
KAVSHELL TRACE /ON /F:"C:\Pasta de Rastreamento" /LVL:warning
```

*Para ativar o log de rastreamento com o uso do nível de detalhe **Eventos importantes**, salve o arquivo de log na pasta C:\Trace Folder, ative a rotação dos arquivos de rastreamento após um número máximo de 50 arquivos de rastreamento ser atingido e execute o seguinte comando:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning /r:50
```

Para desativar o log de rastreamento:

```
KAVSHELL TRACE /OFF
```

Códigos de retorno do comando KAVSHELL TRACE.

Desfragmentação dos arquivos de log do Kaspersky Embedded Systems Security for Windows. KAVSHELL VACUUM

É possível usar o comando `KAVSHELL VACUUM` para desfragmentar os arquivos de log do aplicativo. Isso ajuda a evitar erros de sistema e do aplicativo devido ao armazenamento de um grande número de arquivos de log contendo eventos do aplicativo.

Uma senha pode ser necessária para executar o comando. Para digitar a senha atual, use `[/pwd:<senha>]`.

Recomendamos aplicar o comando `KAVSHELL VACUUM` para otimizar o armazenamento de arquivos de log caso tarefas de Verificação por Demanda e de atualização sejam executadas frequentemente. Esse comando leva o Kaspersky Embedded Systems Security for Windows a atualizar a estrutura lógica dos arquivos de log do aplicativo armazenados em um dispositivo protegido no caminho especificado.

Por padrão, os arquivos de log do aplicativo são armazenados em "C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Reports". Caso tenha especificado manualmente outro caminho para o armazenamento de logs, o comando `KAVSHELL VACUUM` realizará a desfragmentação dos arquivos na pasta especificada nas configurações de log do Kaspersky Embedded Systems Security for Windows.

Tamanhos de arquivo grandes aumentam o tempo necessário para que o comando `KAVSHELL VACUUM` conclua a operação de defragmentação.

As tarefas de Proteção em Tempo Real e de Controle do Computador não estão disponíveis durante a execução do comando `KAVSHELL VACUUM`. O processo de desfragmentação bloqueia o acesso ao log do Kaspersky Embedded Systems Security for Windows e evita o registro de eventos em log. Para evitar a redução da proteção, recomendamos planejar o momento da execução do comando `KAVSHELL VACUUM`.

Para desfragmentar os arquivos de log do Kaspersky Embedded Systems Security for Windows, execute o comando seguinte:

```
KAVSHELL VACUUM
```

Este comando requer direitos da conta do Sistema local.

Limpeza da base iSwift. KAVSHELL FBRESET

O Kaspersky Embedded Systems Security for Windows 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 for Windows cria os arquivos klamfb.dat e klamfb2.dat na pasta "%SYSTEMDRIVE%\System Volume Information". Esses arquivos contêm informações sobre objetos limpos que já foram verificados. O arquivo klamfb.dat (klamfb2.dat) cresce com o número de arquivos verificados pelo Kaspersky Embedded Systems Security for Windows. Ele contém somente informações atuais sobre arquivos no sistema: se um arquivo for removido, o Kaspersky Embedded Systems Security for Windows eliminará as informações correspondentes do klamfb.dat.

Para limpar um arquivo, use o comando `KAVSHELL FBRESET`.

Lembre-se sempre das seguintes instruções ao usar o comando `KAVSHELL FBRESET`:

- Ao usar o comando KAVSHELL FBRESET para limpar o arquivo klamfb.dat, o Kaspersky Embedded Systems Security for Windows não pausa a proteção (ao contrário do que acontece se o klamfb.dat for excluído manualmente).
- O Kaspersky Embedded Systems Security for Windows poderá aumentar a carga de trabalho do dispositivo protegido depois que os dados no klamfb.dat forem limpos. Nesse caso, o Kaspersky Embedded Systems Security for Windows verifica todos os arquivos acessados pela primeira vez após a limpeza do klamfb.dat. Após a verificação, o Kaspersky Embedded Systems Security for Windows coloca informações sobre cada objeto verificado de volta no klamfb.dat. Caso haja novas tentativas de acessar um objeto, a tecnologia iSwift evitará que o arquivo seja verificado novamente caso ele permaneça inalterado.

O comando `KAVSHELL FBRESET` está disponível apenas se o interpretador da linha de comando for iniciado na conta SYSTEM.

Ativação e desativação da criação do arquivo de despejo. KAVSHELL DUMP

É possível utilizar o comando `KAVSHELL DUMP` para ativar ou desativar a criação de snapshots (arquivo de despejo) de processos do Kaspersky Embedded Systems Security for Windows caso sejam encerrados de forma anormal (consulte a tabela a seguir). Além disso, é possível criar um arquivo de despejo de processos do Kaspersky Embedded Systems Security for Windows em execução a qualquer momento.

Para criar um arquivo de despejo com sucesso, o comando `KAVSHELL DUMP` deve ser executado na conta do sistema local (SYSTEM).

O Kaspersky Embedded Systems Security for Windows grava as informações nos arquivos de rastreamento e no arquivo de despejo no formulário não criptografado.

O comando KAVSHELL DUMP não pode ser utilizado para processos x64.

Sintaxe do comando KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<pasta com o arquivo de despejo>|/SNAPSHOT /F:< pasta com o arquivo de despejo> /P:<pid> | /OFF>
```

Parâmetros/opções da linha de comando KAVSHELL DUMP

Chave	Descrição
/ON	Habilita a criação de um arquivo de despejo se um processo for encerrado de forma anormal.
/F:<caminho da pasta com arquivos de despejo>	Esse é um parâmetro obrigatório. Ele especifica o caminho da pasta onde o arquivo de despejo será salvo. Caminhos para pastas nas unidades de rede de outros dispositivos desprotegidos não são permitidos. As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho da pasta para o arquivo de despejo; não são permitidas variáveis do ambiente do usuário.
/SNAPSHOT	Tira um instantâneo da memória do processo em execução com o PID especificado e salva o arquivo de despejo na pasta especificada pelo parâmetro /F.
/P	O identificador do processo (PID) é exibido no Gerenciador de Tarefas do Microsoft Windows.
/OFF	Desabilita a criação de um arquivo de despejo se um processo for encerrado de forma anormal.

Códigos de retorno do comando KAVSHELL DUMP.

Exemplo do comando KAVSHELL DUMP

Para ativar a criação de um arquivo de despejo, salvando o arquivo de despejo na pasta "C:\Pasta de Despejo", execute o comando:

```
KAVSHELL DUMP /ON /F:"C:\Pasta de Despejo"
```

Para gerar 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 criação de arquivos de despejo, execute o comando:

```
KAVSHELL DUMP /OFF
```

Importação das configurações. KAVSHELL IMPORT

O comando `KAVSHELL IMPORT` permite importar as configurações do Kaspersky Embedded Systems Security for Windows e suas tarefas atuais a partir de um arquivo de configuração para uma cópia do Kaspersky Embedded Systems Security for Windows no dispositivo protegido. É possível criar um arquivo de configuração usando o comando `KAVSHELL EXPORT`.

Uma senha pode ser necessária para executar o comando. Para digitar a senha atual, use `[/pwd:<senha>]`.

Sintaxe do comando KAVSHELL IMPORT

```
KAVSHELL IMPORT <nome do arquivo de configuração e caminho do arquivo>
```

Exemplos do comando KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Parâmetros da linha de comando KAVSHELL IMPORT

Configuração	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.

Exportação das configurações. KAVSHELL EXPORT

O comando `KAVSHELL EXPORT` permite exportar todas as configurações do Kaspersky Embedded Systems Security for Windows e suas tarefas atuais para um arquivo de configuração para, depois, importá-las para cópias do Kaspersky Embedded Systems Security for Windows instaladas em outro dispositivo protegido.

Sintaxe do comando KAVSHELL EXPORT

```
KAVSHELL EXPORT <nome do arquivo de configuração e caminho do arquivo>
```

Exemplos do comando KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Parâmetros da linha de comando KAVSHELL EXPORT

Configuração	Descrição
<nome do arquivo de configuração e caminho do arquivo>	Nome do arquivo de configuração que conterá as configurações. É possível atribuir qualquer extensão de arquivo 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.

Integração com Microsoft Operations Management Suite. KAVSHELL OMSINFO

O comando KAVSHELL OMSINFO permite analisar o status do aplicativo e as informações sobre as ameaças detectadas pelos bancos de dados de antivírus. As informações sobre ameaças são tiradas 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
```

Parâmetros da linha de comando KAVSHELL OMSINFO

Configuração	Descrição
<caminho do arquivo gerado com nome de arquivo>	Nome do arquivo gerado que conterá informações sobre o status de aplicativo e qualquer ameaça detectada.

Gerenciando a tarefa do Monitor de Comparação de Integridade de Arquivos: KAVSHELL FIM /BASELINE

É possível utilizar o comando `KAVSHELL FIM /BASELINE` para configurar o modo no qual a tarefa do Monitor de Comparação de Integridade de Arquivos executa e monitora o carregamento de módulos DLL.

Uma senha pode ser necessária para executar o comando. Para digitar a senha atual, use `[/pwd:<senha>]`.

Sintaxe do comando KAVSHELL FIM /BASELINE

```
KAVSHELL FIM /BASELINE [/CREATE: [<escopo de monitoramento> | /L:<caminho para o arquivo TXT contendo a lista de escopos de monitoramento>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<id de linha de base> | /ALIAS:<alias existente>]] | [/EXPORT:<caminho para arquivo TXT> [/BL:<id de linha de base> | /ALIAS:<alias existente>]] | [/SHOW [/BL:<id de linha de base> | /ALIAS:<alias existente>]] | [/SCAN [/BL:<id de linha de base> | /ALIAS:<alias existente>]] | [/PWD:<senha>]
```

Exemplos do comando KAVSHELL FIM /BASELINE

Para excluir uma linha de base, execute o seguinte comando:

```
KAVSHELL FIM /BASELINE /CLEAR /BL:<id de linha de base>
```

É possível definir as configurações da tarefa do Monitor de comparação de Integridade de Arquivos usando as opções de linha de comando (consulte a tabela abaixo).

Parâmetros/opções da linha de comando `KAVSHELL FIM /BASELINE`

Parâmetro/opção	Descrição
`/CREATE`	Crie uma nova tarefa do Monitor de Comparação de Integridade de Arquivos. O Kaspersky Embedded Systems Security for Windows iniciará a nova tarefa do Monitor de Comparação de Integridade de Arquivos para criar uma linha de base.
`/L`	Especifique o caminho para o arquivo TXT que contém a lista de escopos de monitoramento.
`/MD5`	Especifique o algoritmo MD5 para calcular uma soma de verificação (parâmetro opcional). Parâmetro `/MD5` não pode ser usado junto com `/SHA256`. O algoritmo MD5 é usado por padrão.
`/SHA256`	Especifique o algoritmo SHA256 para calcular uma soma de verificação (parâmetro opcional). O parâmetro `/SHA256` não pode ser utilizado juntamente com o `/MD5`. O algoritmo MD5 é usado por padrão.
`/SF`	Inclui todas as subpastas no escopo da tarefa do Monitor de Comparação de Integridade de Arquivos (parâmetro opcional). Por padrão, todas as subpastas são excluídas do escopo da tarefa do Monitor de Comparação de Integridade de Arquivos.
`/CLEAR`	Exclua a linha de base com a `<id de linha de base>` especificada ou a linha de base da tarefa com o `<alias existente>` especificado. Exclua todas as linhas de base se nem um `<id de linha de base>` nem um `<alias existente>` tiver sido especificado. Parâmetro opcional.
`/BL`	Especifique o ID exclusivo de uma linha de base (parâmetro

	opcional).
`/EXPORT`	Exporte os dados sobre todas as linhas de base em um arquivo TXT.
`/SHOW`	Mostrar os dados sobre todas as linhas de base.
`/SCAN`	Inicie a tarefa do Monitor de Comparação de Integridade de Arquivos com `<id de linha de base>` especificada ou `<alias existente>` especificado.
`/ALIAS`	Especifique o nome de uma tarefa existente ou o nome de uma nova tarefa.
`<escopo de monitoramento>`	Especifique o arquivo ou a pasta que deseja incluir no escopo da tarefa do Monitor de Comparação de Integridade de Arquivos. Este parâmetro permite especificar apenas uma área.
`<caminho para o arquivo TXT contendo a lista de escopos de monitoramento>`	Especifique o caminho para o arquivo TXT que contém a lista de escopos de monitoramento. O arquivo deve ter UTF-8 codificado e cada caminho para um escopo de monitoramento deve ser especificado em uma linha separada.
`<caminho para arquivo TXT>`	Especifique o caminho para o arquivo para o qual você deseja exportar os dados sobre todas as linhas de base.
`<id de linha de base>`	Especifique o ID exclusivo de uma linha de base. Você pode usar o parâmetro `/SHOW` para conhecer o ID de uma linha de base.
`<alias existente>`	Especifique o nome de uma tarefa existente.
`<novo alias>`	Especifique o nome de uma nova tarefa.

Códigos de retorno do comando

Código de retorno dos comandos KAVSHELL START e KAVSHELL STOP

Código de retorno dos comandos KAVSHELL START e KAVSHELL STOP

Código de retorno	Descrição
0	Operação concluída com êxito
-3	Erro de permissão
-5	Sintaxe de comando inválida
-6	Operação inválida (por exemplo, o Kaspersky Security Service 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 dispositivo protegido em outra conta de usuário falhou (por padrão,

	Kaspersky Security Service é executado na conta de usuário do sistema local)
-99	Erro desconhecido

Código de retorno dos comandos KAVSHELL SCAN e KAVSHELL SCANCRITICAL

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 permissão
-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 log de tarefas
-99	Erro desconhecido
-301	Chave inválida

Código de retorno do comando KAVSHELL TASK LOG-INSPECTOR

Código de retorno do comando KAVSHELL TASK LOG-INSPECTOR

Código de retorno	Descrição
0	Operação concluída com êxito
-6	Operação inválida (por exemplo, o Kaspersky Security Service já está em execução ou já foi interrompido)
402	A tarefa já está em execução (para a opção /STATE)

Códigos de retorno do comando KAVSHELL TASK

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 permissão
-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	A tarefa não está sendo executada (para a opção /STATE)
402	A tarefa já está em execução (para a opção /STATE)
403	Tarefa já pausada (para a opção /STATE)
-404	Falha na operação (uma alteração no status da tarefa resultou em travamento)

Códigos de retorno do comando KAVSHELL RTP

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 permissão
-4	Objeto não encontrado (uma ou todas as tarefas de Proteção do Computador em Tempo Real não foram 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

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 permissão
-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 ao Kaspersky Security Center
-235	O Kaspersky Embedded Systems Security for Windows não foi autenticado ao conectar a fonte de atualização
-236	O banco de dados do aplicativo está corrompido
-301	Chave inválida

Códigos de retorno do comando KAVSHELL ROLLBACK

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 permissão
-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

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

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 permissão
-4	Objeto não encontrado (caminho especificado 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 quando os logs de despejo já estão desativados)
-99	Erro desconhecido

Códigos de retorno do comando KAVSHELL FBRESET

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

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 permissão
-4	Objeto não encontrado (caminho especificado 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

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 permissão
-4	Objeto não encontrado (não foi possível encontrar um arquivo de configuração que possa ser importado)
-5	Sintaxe inválida
-99	Erro desconhecido
501	Operação concluída com êxito mas com um erro/comentário; por exemplo, o Kaspersky Embedded Systems Security for Windows não importou parâmetros de algum componente funcional
-502	Arquivo de importação ausente ou em 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 for Windows)

Códigos de retorno do comando KAVSHELL EXPORT

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 permissão
-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 mas com um erro/comentário; por exemplo, o Kaspersky Embedded Systems Security for Windows não exportou parâmetros de algum componente funcional

Códigos de retorno do comando KAVSHELL FIM /BASELINE

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissão
-4	Objeto não encontrado (tarefa não encontrada)
-5	Sintaxe de comando inválida
-6	Operação inválida (por exemplo, a linha de base já foi excluída)
-10	Não foi possível criar um arquivo de configuração (por exemplo, não existe acesso à pasta especificada no caminho para o arquivo)
-12	Senha inválida
-80	Inconsistente com os objetos de linha de base detectados
-85	Falha ao criar o log de tarefas
-99	Erro interno
-303	Chave de licença inválida
-502	A tarefa não está em execução
200	Todos os objetos são consistentes com a linha de base
501	Tarefa concluída com sucesso com um erro/comentário

Entrando em contato com o Suporte Técnico

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

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 recomendado 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.

O suporte ao aplicativo é fornecido de acordo com seu ciclo de vida (consulte a página do ciclo de vida do aplicativo).

Antes de entrar em contato com o Suporte Técnico, leia todas as regras do Suporte Técnico.

É possível entrar em contato enviando uma solicitação ao Suporte Técnico da Kaspersky por meio do portal Kaspersky CompanyAccount.

Suporte Técnico por meio do Kaspersky CompanyAccount

O Kaspersky CompanyAccount é um portal para as empresas que utilizam os aplicativos da Kaspersky. O Kaspersky CompanyAccount destina-se a facilitar a interação entre os usuários e os especialistas do Kaspersky através de solicitações online. Com o Kaspersky CompanyAccount, é possível monitorar o andamento do processamento de solicitações eletrônicas pelos especialistas da Kaspersky, além de 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 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.

Usando arquivos de rastreamento e scripts do AVZ

Após você reportar um problema aos especialistas de Suporte Técnico da Kaspersky, eles poderão solicitar que você crie um relatório com informações sobre a operação do Kaspersky Embedded Systems Security for Windows e que o envie ao Suporte Técnico da Kaspersky. Além disso, os especialistas do Suporte Técnico da Kaspersky 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 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 dispositivo protegido para detectar ameaças, desinfectar ou excluir arquivos infectados e criar relatórios de verificação do sistema.

Glossário

Analisador heurístico

Tecnologia de detecção de ameaças cujas informações ainda não foram adicionadas aos bancos de dados da Kaspersky. 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, esses são arquivos executáveis, com extensões do tipo .com, .exe, .dll entre outras. O risco de que um código malicioso invada esses arquivos é bastante alto.

Atualização

O processo de substituição ou adição de novos arquivos (bancos de dados ou módulos do aplicativo) recuperados de servidores de atualização da Kaspersky.

Backup

Armazenamento especial destinado a salvar cópias de backup de objetos antes que eles sejam desinfectados ou excluídos.

Bancos de dados de Antivírus

Bancos de dados que contêm informações sobre ameaças à segurança do computador conhecidas pela Kaspersky na data de lançamento dos bancos de dados de antivírus. As entradas do banco de dados de antivírus possibilitam a detecção de código malicioso em objetos verificados. Os bancos de dados de antivírus são criados pelos especialistas da Kaspersky e atualizados de hora em hora.

Chave ativa

Uma chave que está sendo usada atualmente pelo aplicativo.

Configurações de tarefa

Configurações específicas do aplicativo para cada tipo de tarefa.

Desinfecção

Método de processamento de objetos infectados que resulta na recuperação completa ou parcial dos dados. Nem todos os objetos infectados podem ser desinfectados.

Estado de proteção

O status de proteção atual que caracteriza o nível de segurança do dispositivo.

Falso positivo

Uma situação na qual o aplicativo da Kaspersky considera um objeto não infectado como infectado devido à semelhança de seu código com o código de um vírus.

Importância do evento

Propriedade de um evento encontrado durante a operação de um aplicativo da Kaspersky. Existem quatro níveis de importância:

- Evento crítico.
- Falha funcional.
- Aviso.
- Informação.

Os eventos do mesmo tipo podem ter níveis de importância diferentes dependendo da situação na qual o evento ocorreu.

Kaspersky Security Network (KSN)

Infraestrutura de serviços em nuvem que fornece acesso à base de dados de conhecimento on-line da Kaspersky sobre a reputação de arquivos, recursos da Web e software. Usar os dados da Kaspersky Security Network garante respostas mais rápidas por aplicativos da Kaspersky contra ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos.

Máscara de arquivos

Uma representação de um nome de arquivo que usa caracteres genéricos. Os principais caracteres usados em máscaras de arquivos são * e ?, (onde * significa qualquer número de caracteres e ? significa qualquer caractere).

Nível de segurança

Um nível de segurança é um conjunto predefinido de configurações do componente.

Objeto infectado

Um objeto no qual uma seção de código corresponde completamente a uma seção de código de uma ameaça conhecida. Os especialistas da Kaspersky não recomendam trabalhar com esses 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.

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.

Período da licença

O período de tempo durante o qual é possível usar as funções do aplicativo e os serviços adicionais. O escopo dos recursos disponíveis e dos serviços adicionais depende do tipo de licença.

Política

Uma política define as configurações de um aplicativo e gerencia a capacidade de configurar o aplicativo em computadores dentro de um grupo de administração. Uma política individual deve ser criada para cada aplicativo. É possível criar diversas 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.

Quarentena

A pasta para onde o aplicativo da Kaspersky move objetos possivelmente infectados que foram detectados. Os objetos são armazenados na Quarentena em formato criptografado para evitar qualquer impacto negativo no computador.

Servidor de Administração

Um componente do Kaspersky Security Center que armazena as informações sobre os aplicativos da Kaspersky instalados na rede corporativa e que os gerencia.

SIEM

Uma abreviação de Informações de Segurança e Gerenciamento de Eventos. Uma solução para gerenciar informações e eventos no sistema de segurança de uma organização.

Tarefa

As funções executadas pelo aplicativo da Kaspersky são implementadas como tarefas, por exemplo: Proteção de Arquivos em Tempo Real e Atualização do Banco de Dados.

Tarefa local

Uma tarefa definida e executada em um computador cliente individual.

Vulnerabilidade

Uma falha no sistema operacional ou em um aplicativo que pode ser explorada por desenvolvedores de malwares para penetrar no sistema operacional ou em aplicativos e corromper sua integridade. A presença de um grande número de vulnerabilidades em um sistema operacional o torna pouco confiável, uma vez que os vírus que penetrarem nele poderão causar problemas no sistema operacional e nos aplicativos instalados.

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.

Domino, Lotus e Lotus Notes são marcas comerciais registradas da International Business Machines Corporation, registradas em muitas jurisdições do mundo.

Intel e Pentium são marcas registradas da Intel Corporation nos Estados Unidos e/ou em outros países.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e em outros países.

Microsoft, Active Directory, Excel, Forefront, Hyper-V, Internet Explorer, JScript, Lync, PowerShell, Outlook, SharePoint, SQL Server, Windows, Windows Server, Windows Vista, Windows XP são marcas comerciais registradas do grupo de empresas Microsoft.

CVE é uma marca registrada de The MITRE Corporation.

UNIX é uma marca registrada nos Estados Unidos e em outros países, licenciada exclusivamente pela X/Open Company Limited.