kaspersky

Kaspersky Embedded Systems Security 4.0 for Windows

© 2025 AO Kaspersky Lab

Índice

Kaspersky Embedded Systems Security for Windows
- O que há de novo
- Kit de distribuição
- Requisitos de hardware e software
- Versões compatíveis do Kaspersky Security Center
- Requisitos e limitações funcionais
  - Instalar e remover o aplicativo
  - Monitor de integridade do sistema
  - Firewall
  - Limitações em versões desatualizadas do Windows
  - Integração com o Kaspersky Security Center
  - Outras limitações
- Compatibilidade com outros aplicativos

Instalar e remover o aplicativo
- Planejamento da instalação
  - Seleção das ferramentas de administração
  - Seleção do tipo de instalação
- Instalação e desinstalação do aplicativo usando um assistente
  - Instalação usando o Assistente de instalação
    - Instalação do Kaspersky Embedded Systems Security
    - Instalação do Console do Kaspersky Embedded Systems Security
    - Configurações avançadas após a instalação do Console do Aplicativo em outro dispositivo
      - Permitir o acesso remoto anônimo a aplicativos COM
      - Permitir conexões de rede para o processo de gerenciamento remoto do Kaspersky Embedded Systems Security
    - Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security
      - Inicialização e configuração da tarefa de atualização de bancos de dados e módulos do aplicativo
      - Verificação de Áreas Críticas
  - Alteração do conjunto de componentes e reparação do Kaspersky Embedded Systems Security
  - Desinstalação usando o Assistente de instalação
    - Desinstalação do Kaspersky Embedded Systems Security
    - Desinstalação do Console do Kaspersky Embedded Systems Security
- Instalação e desinstalação do aplicativo a partir da linha de comando
  - Sobre a instalação e desinstalação do Kaspersky Embedded Systems Security a partir da linha de comando
  - Códigos de componentes de software do Kaspersky Embedded Systems Security para o serviço do Windows Installer
    - Componentes de software do Kaspersky Embedded Systems Security
    - Componente do software "ferramentas de administração"
  - Configurações de instalação e recuperação e opções de linha de comando do Windows Installer
  - Exemplos de comandos para instalar o Kaspersky Embedded Systems Security
  - Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security
  - Adicionar/remover componentes. Exemplos de comandos
  - Desinstalação do Kaspersky Embedded Systems Security. Exemplos de comandos
  - Códigos de retorno

Instalação e desinstalação do aplicativo usando o Kaspersky Security Center
Informações gerais sobre a instalação por meio do Kaspersky Security Center
Direitos para instalar ou desinstalar o Kaspersky Embedded Systems Security
Instalação do Kaspersky Embedded Systems Security através do Kaspersky Security Center
Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security
Instalação do Console do Aplicativo por meio do Kaspersky Security Center
Desinstalação do Kaspersky Embedded Systems Security através do Kaspersky Security Center
Alterar o conjunto de componentes de componentes de aplicativos usando o Kaspersky Security Center
Instalação e desinstalação via políticas de grupo do Active Directory
Instalação do Kaspersky Embedded Systems Security através das políticas de grupo do Active Directory
Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security
Desinstalação do Kaspersky Embedded Systems Security através das políticas de grupo do Active Directory
Logs de instalação e desinstalação do Kaspersky Embedded Systems Security
Modificações de sistema após a instalação do Kaspersky Embedded Systems Security
Processos do Kaspersky Embedded Systems Security
Verificação das funções do Kaspersky Embedded Systems Security. Uso do vírus de teste EICAR
Sobre o vírus de teste EICAR
Verificação dos recursos de Proteção de Arquivos em Tempo Real e Verificação por Demanda
Atualizar versões antigas do Kaspersky Embedded Systems Security para a versão 4.0
Atualização do Kaspersky Embedded Systems Security
Atualização das Ferramentas de Administração do Kaspersky Embedded Systems Security
Migrar as políticas e tarefas
Migração das configurações da versão do aplicativo que está sendo atualizada
Correspondência de componentes e tarefas no Kaspersky Embedded Systems Security versões 3.4 e 4.0
Interface do aplicativo
Trabalhar com o Plug-in de Administração
Gerenciamento do Kaspersky Embedded Systems Security a partir do Kaspersky Security Center
Gerenciamento das configurações do aplicativo
Navegação
Abertura das configurações gerais na janela de propriedades do aplicativo
Abertura das configurações gerais por meio da política
Definição das configurações gerais do aplicativo no Kaspersky Security Center
Definição das configurações de escalabilidade, interface e verificação no Kaspersky Security Center
Definição das configurações de segurança no Kaspersky Security Center
Definição das configurações de conexão usando o Kaspersky Security Center
Configuração da inicialização programada de tarefas locais do sistema
Definição das configurações de segurança no Kaspersky Security Center
Criação e configuração de políticas
Criar uma política
Configuração de políticas
Indicador do nível de segurança
Criando e configurando uma tarefa usando o Kaspersky Security Center
Sobre a criação de tarefa no Kaspersky Security Center
Criação de uma tarefa usando o Kaspersky Security Center
Acesso a configurações da tarefa local e configurações gerais do aplicativo para um computador individual

Configurando tarefas de grupo no Kaspersky Security Center
Status da ativação do aplicativo.
Tarefa de atualização
Controle de integridade de aplicativos
Gerenciando programações de tarefas
Programação de tarefas
Ativando e desativando tarefas programadas
Relatórios no Kaspersky Security Center
Trabalhar com o Console do Kaspersky Embedded Systems Security
Abrir o Console do Aplicativo
Interface do Console do Kaspersky Embedded Systems Security
Janela do Console do Kaspersky Embedded Systems Security
Ícone da Bandeja do Sistema na área de notificação
Definindo as configurações de log por meio do Console do Aplicativo
Gerenciando as tarefas do Kaspersky Embedded Systems Security
Categorias de tarefa do Kaspersky Embedded Systems Security
Executar, pausar, reiniciar e interromper tarefas manualmente
Gerenciando programações de tarefas
Definição das configurações da programação da tarefa
Ativando e desativando tarefas programadas
Uso de contas de usuário para iniciar tarefas
Sobre como usar contas para iniciar tarefas
Especificação de uma conta de usuário para iniciar uma tarefa
Configurações de importação e exportação
Sobre a importação e exportação de configurações
Exportando configurações
Importando configurações
Visualizando o status de proteção e as informações do Kaspersky Embedded Systems Security
Trabalhando com o plug-in da Web a partir do Web Console e Cloud Console
Gerenciamento do Kaspersky Embedded Systems Security a partir do Web Console e Cloud Console
Limitações do Plug-in da Web
Gerenciamento das configurações do aplicativo
Definição das configurações gerais do aplicativo no plug-in da Web
Definição das configurações de escalabilidade, interface e verificação no plug-in da Web
Definição das configurações de segurança no plug-in da Web
Definição das configurações de conexão no plug-in da Web
Configuração da inicialização agendada de tarefas locais no plug-in da Web
Definição das configurações de conexão no plug-in da Web
Criação e configuração de políticas
Criando e configurando uma tarefa usando o Kaspersky Security Center
Sobre a criação de tarefas no plug-in da Web
Criação de uma tarefa no plug-in da Web
Configuração de tarefas de grupo no plug-in da Web
Configuração da tarefa de ativação do aplicativo no plug-in da Web
Configuração das tarefas de Atualização no plug-in da Web

Gerenciando programações de tarefas
Programação de tarefas
Ativando e desativando tarefas programadas
Relatórios no Kaspersky Security Center
Licenciamento do aplicativo
Sobre o Contrato de Licença do Usuário Final
Sobre a licença
Sobre o certificado da licença
Sobre a chave
Sobre o arquivo de chave
Sobre o código de ativação
Comparação da funcionalidade do aplicativo dependendo do tipo de licença
Ativar o aplicativo com um arquivo de chave
Ativação do aplicativo com um código
Visualização das informações sobre a licença atual
Renovação da licença
Exclusão da chave
Sobre a coleta de dados
Conformidade com a legislação da União Europeia (GDPR)
Inicialização e interrupção do Kaspersky Embedded Systems Security
Iniciando e interrompendo o aplicativo
Pausar e reiniciar a Proteção e Controle do computador
Interface de diagnóstico compacta
Sobre a interface de diagnóstico compacta
Revisão do status do Kaspersky Embedded Systems Security por meio da Interface de diagnóstico compacta
Revisando estatística de evento de segurança
Revisando a atividade atual do aplicativo
Configurando o rastreamento do aplicativo e registro do despejo de memória
Autodefesa do Kaspersky Embedded Systems Security
Ativar ou desativar a Autodefesa
Compatibilidade com a tecnologia AM-PPL
Proteção de serviços do sistema operacional
Configuração de permissões de usuário para gerenciar o Kaspersky Embedded Systems Security
Configuração de permissões de acesso de usuários para gerenciar o Kaspersky Security Service
Acesso protegido por senha às funções do Kaspersky Embedded Systems Security
Notificações do Secure Desktop
Zona confiável
Criar uma exclusão de verificação
Selecionar tipos de objetos detectáveis
Editar a lista de aplicativos confiáveis
Criando uma zona confiável local
Exportar e importar a zona confiável
Usar armazenamento de certificado de sistema confiável
Proteção de Arquivos em Tempo Real
Sobre o escopo de proteção da tarefa e configurações de segurança
Escopos da proteção predefinidos
Sobre níveis de segurança predefinidos

- Extensões de arquivos verificadas por padrão na tarefa de Proteção de Arquivos em Tempo Real
- Configuração da tarefa de Proteção de Arquivos em Tempo Real
- Configurando o escopo de proteção para o componente de Proteção de Arquivos em Tempo Real
- Definição manual de configurações de segurança
- Verificação de contêineres

Uso da KSN
- Ativação do uso da Kaspersky Security Network
- Estatísticas de uso da Kaspersky Security Network
- Limitações da Kaspersky Private Security Network
- Configurações de proxy da KSN

Prevenção de Exploit
- Modo de Prevenção de Exploits
- Ativar e desativar a Prevenção de Exploit
- Ativar e desativar a proteção da memória
- Criar uma lista de processos confiáveis.

Mecanismo de Remediação

Detecção de Comportamento
- Ativação e desativação da proteção por criptografia para pastas locais
- Proteção de pastas compartilhadas contra criptografia externa
  - Ativar e desativar a proteção de pastas compartilhadas contra criptografia externa
  - Criação do escopo da proteção
  - Adicionar computadores confiáveis para criptografia externa de dados
  - Configurar o período de bloqueio de um computador não confiável
  - Exportar e importar uma lista de exclusões da proteção de pastas compartilhadas contra criptografia externa

Proteção Contra Ameaças à Rede

Scanner AMSI
- Ativar e desativar a proteção AMSI
- Configurações de Proteção AMSI

Controle de Inicialização de Aplicativos
- Sobre as regras do Controle de Inicialização de Aplicativos
- Sobre o Controle de Distribuição de Software
- Sobre o Gerador de Regras de Controle de Inicialização de Aplicativos
- Ativando e configurando o Controle de Inicialização de Aplicativos
- Configuração do controle de distribuição de software
- Trabalhar com a lista de regras de Controle de Inicialização de Aplicativos
  - Adição de uma regra de Controle de Inicialização de Aplicativos
  - Adicionar uma condição de acionamento para a regra de Controle de Aplicativos
  - Adição de exclusões a partir de um escopo de regra de Controle de Inicialização de Aplicativos
  - Ativar o modo de Permissão padrão
  - Gerando um arquivo TXT com uma seleção de eventos de aplicativo bloqueado pelo Kaspersky Security Center
- Configuração de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos
- Usando uma tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos.

Controle de Dispositivos
- Regras de acesso do dispositivo
- Controle de acesso de dispositivos por tipo
- Controle de conexões Wi-Fi
- Controle de impressão

Entrada do controle de dispositivos (HID)
Monitorar o uso de unidades removíveis
Gerenciando o acesso a dispositivos Bluetooth
Diferenciação dos direitos de acesso do usuário aos dispositivos
Auditoria de dispositivo externa
Adicionar processos confiáveis
Exportação e importação da lista de dispositivos confiáveis
Firewall
Sobre as Regras de Firewall
Configurando o Firewall
Definir configurações gerais de tarefas
Criação e configuração das regras de Firewall
Como ativar e desativar as regras de Firewall
Prevenção contra ataque BadUSB
Monitor de integridade do sistema
Sobre as regras do monitor de integridade do sistema
Monitor de integridade do sistema em tempo real
Verificação de integridade do sistema sob demanda
Exportação e importação das regras do monitor de integridade do sistema
Visualização de relatórios do monitor de integridade do sistema
Inspeção do Log
Adição de regras personalizadas
Configuração de regras predefinidas
Verificação sob demanda
Sobre tarefas de Verificação por Demanda
Sobre o escopo da verificação e configurações de segurança da tarefa
Escopos de verificação predefinidos
Verificação de arquivos no armazenamento on-line
Sobre níveis de segurança predefinidos
Verificação de unidades removíveis
Configurações padrão das tarefas de Verificação por Demanda
Sobre tarefas de Verificação por Demanda
Navegação
Abertura do assistente da tarefa de Verificação por Demanda
Abertura das configurações da tarefa de Verificação por Demanda
Criando uma tarefa de Verificação por Demanda
Execução de uma tarefa de Verificação por Demanda em segundo plano
Registrando a execução de uma Verificação de Áreas Críticas
Configurando o escopo da verificação na tarefa Verificação por Demanda
Abertura das configurações da tarefa de Verificação por Demanda
Configuração da Verificação de Unidades Removíveis
Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda
Definição manual de configurações de segurança
Estatísticas da tarefa de Verificação por Demanda
Atualização do banco de dados e dos módulos de software do Kaspersky Embedded Systems Security
Atualizar bancos de dados e módulos do software aplicativo
Sobre as tarefas de atualização

- Esquemas de atualização do banco de dados e dos módulos de software do Kaspersky Embedded Systems Security
- Configurando tarefas de atualização
- Atualização SMU do aplicativo
- Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security
- Estatísticas da tarefa de atualização

Como fazer cópias de backup de objetos

- Como fazer cópias de backup de objetos. Backup
  - Visualizando objetos armazenados no Backup
    - Classificando arquivos no Backup
    - Filtrando arquivos no Backup
  - Restaurando arquivos do Backup
  - Excluindo arquivos do Backup
  - Envio de objetos possivelmente infectados à Kaspersky para análise
  - Configurando o Backup
  - Estatísticas do backup
- Bloqueio do acesso aos recursos da rede. Sessões de rede bloqueadas
  - Lista de sessões de rede bloqueadas
  - Migrando a lista de sessões de rede bloqueadas

Registro de eventos. Logs do Kaspersky Embedded Systems Security

- Modos para registrar eventos do Kaspersky Embedded Systems Security
- Definir as configurações de log
  - Classificação de eventos no log
  - Filtragem de eventos no log
  - Exclusão de eventos do log
  - Exportação de informações do log
- Log de auditoria do sistema
- Logs de tarefas
  - Visualizando estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security em logs de tarefas
- Visualizando o log de eventos do Kaspersky Embedded Systems Security no Visualizador de eventos
- Sobre a integração SIEM
  - Definições das configurações de integração SIEM
- Métodos de notificação do administrador e dos usuários
  - Configurando notificações do administrador e dos usuários
  - Configuração de notificações por e-mail
- Configuração de interações com o Servidor de Administração

Managed Detection and Response

- Configurações de integração MDR

Entrar em contato com o Suporte Técnico

- Como obter suporte técnico
- Suporte Técnico por meio do Kaspersky CompanyAccount
- Oferecendo informações de diagnóstico estendidas aos especialistas do Suporte Técnico
- Rastreamento de funcionamento do aplicativo
- Registro dos despejos de memória

Fontes de informação sobre o Kaspersky Embedded Systems Security

Glossário

- Analisador heurístico
- Arquivo compactado

- Arquivo infectável
- Atualização
- Backup
- Bancos de dados de Antivírus
- Chave ativa
- Configurações de tarefa
- Desinfecção
- Estado de proteção
- Falso positivo
- Importância do evento
- Kaspersky Security Network (KSN)
- Máscara de arquivos
- Nível de segurança
- Objeto infectado
- Objeto OLE
- Objetos de inicialização
- Período da licença
- Política
- Quarentena
- Servidor de Administração
- SIEM
- Tarefa
- Tarefa local
- Vulnerabilidade

Informações sobre código de terceiros

Avisos de marcas registradas

Apêndices

- Extensões de arquivo para verificação rápida
- Contas de usuário em regras de componentes de aplicativos

Kaspersky Embedded Systems Security for Windows

O Kaspersky Embedded Systems Security for Windows (doravante referido como Kaspersky Embedded Systems Security) protege computadores e outros sistemas integrados do Microsoft® Windows® (doravante também referidos como dispositivos protegidos) contra vírus e outras ameaças de computador. Os usuários do Kaspersky Embedded Systems Security 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 recomendado usar o aplicativo Kaspersky Industrial CyberSecurity for Nodes.

Você pode instalar o Kaspersky Embedded Systems Security 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 pode ser gerenciado das seguintes formas:

- Por meio do Console do Aplicativo instalado no mesmo dispositivo protegido em que o Kaspersky Embedded Systems Security 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.

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

Componentes e funções do Kaspersky Embedded Systems Security

O aplicativo inclui os seguintes componentes:

- **Proteção de Arquivos em Tempo Real**. O Kaspersky Embedded Systems Security verifica objetos quando eles são acessados. O Kaspersky Embedded Systems Security 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 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.

- **Firewall**. Dependendo do modo selecionado, o componente: monitora a filtragem de tráfego pelo Firewall do Windows; registra no log apenas eventos relacionados à atividade de rede do computador protegido; ou filtra o tráfego de rede com base nas configurações do Firewall.

- **Monitor de Integridade de Arquivos**. O Kaspersky Embedded Systems Security 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 de 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 de bancos de dados e módulos do aplicativo**. O Kaspersky Embedded Systems Security 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 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 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 para um arquivo de configuração XML e importar configurações para o Kaspersky Embedded Systems Security 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.

- **Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security**. É possível configurar os direitos para gerenciar o Kaspersky Embedded Systems Security 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 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 e informações necessárias para o diagnóstico de erros no Kaspersky Embedded Systems Security.

- **Zona confiável**. É possível gerar uma lista de exclusões do escopo da verificação ou da proteção que será aplicada pelo Kaspersky Embedded Systems Security 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.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no programa nos EUA

O que há de novo

O Kaspersky Embedded Systems Security 4.0 oferece os seguintes recursos e melhorias:

- Interface do usuário significativamente atualizada do Console do Aplicativo e os plug-ins para gerenciar o aplicativo usando o Kaspersky Security Center.
- Suporte para Windows 11 24H2.
- Agora você pode alterar a porta que o Console do Aplicativo usa para se conectar a um computador com o aplicativo instalado.
- Na *Zona confiável*, você pode:
  - Configurar processos confiáveis de forma mais granular.
  - Usar o armazenamento confiável de certificados.
- Novas configurações para direitos de usuário e grupo para gerenciar o aplicativo.
- Novo componente *Anti-Rootkit*. Por padrão, o componente é ativado se a *Proteção de arquivos em tempo real* estiver ativada. Você pode desativar o componente durante a instalação do aplicativo, usando a tarefa *Alterar componentes de aplicativo do Kaspersky Embedded Systems Security* ou nas propriedades do pacote de instalação do aplicativo.
- Nas configurações de *Prevenção de Exploits*, o aplicativo agora pode identificar processos protegidos automaticamente.
- Novo componente *Mecanismo de Remediação*.
- O componente Proteção Contra Ameaças à Rede pode monitorar o tráfego de rede para detectar a verificação de portas e solicitações de rede de alta intensidade.
- O aplicativo agora é compatível com o Firewall do Windows. Não é mais necessário remover o Firewall do Windows para instalar o aplicativo.
- O componente *Detecção de Comportamento* monitora pastas compartilhadas, bem como pastas locais.

- Componente reprojetado *Controle de Inicialização de Aplicativos*:
  - Alterações significativas na estrutura das configurações do componente.
  - Para especificar as condições de acionamento e exclusões da regra do Controle de Inicialização de Aplicativos, agora você pode usar o tipo de unidade, categorias KL, grupos KSN.
- Componente reprojetado *Controle de dispositivos*:
  - Por padrão, o componente *Controle de dispositivos* está configurado para permitir a conexão de todos os dispositivos.
  - O *Controle de Wi-Fi* não é mais um componente separado e agora faz parte do Controle de dispositivos.
  - A possibilidade de controlar dispositivos conectados dependendo do barramento de conexão foi adicionada.
  - A migração de configurações para acesso a unidades removíveis foi adicionada durante atualização de versões anteriores do aplicativo para a versão 4.0.
- O componente *Gerenciamento de Firewall* foi reprojetado no componente *Firewall*, que, além de fazer a interface com o firewall do Windows, agora também funciona como um firewall.
- A funcionalidade dos componentes *Monitor de Integridade de Arquivos* e do *Monitoramento de Acesso ao Registro* foi mesclada no novo componente *Monitor de Integridade do Sistema*. Essa melhoria permite rastrear com eficiência as alterações no sistema de arquivos e no registro do Windows, aumentando a proteção contra modificação não autorizada de dados.
- O aplicativo não tem suporte para o agendamento de componentes individuais. Se os componentes forem ativados, eles continuarão em execução enquanto o aplicativo estiver em execução.
- Agora há suporte para o Kaspersky Security Center Windows 15.1.
- Tarefas de grupo adicionadas:
  - *Proteção da conexão do Servidor de Administração*
  - *Alteração do conjunto de componentes do Kaspersky Embedded Systems Security*
  - *Monitor de Integridade do Sistema de linha de base* em vez de *Monitor de Integridade de Arquivos de linha de base*
  - *Atualização* em vez de *Copiar atualizações*, *Atualização do banco de dados do aplicativo* e *Atualização de módulos de software*
  - *Reversão de atualização* em vez de *Reversão de atualização do banco de dados do aplicativo*
  - *Remover a chave*

- O aplicativo verifica a configuração dos componentes de controle antes de salvar as configurações. A verificação foi adicionada para os componentes Controle de Inicialização de Aplicativos, Controle de Dispositivos e Monitor de Integridade do Sistema. Agora, o aplicativo exibe um aviso se as configurações atuais do componente de controle aumentarem a possibilidade de carga ou causarem falhas no sistema do computador. Por exemplo, no caso do Controle de Inicialização de Aplicativos, caso o modo que bloqueia todos os aplicativos seja selecionado, exceto os aplicativos permitidos, e caso nenhuma regra de permissão tenha sido adicionada, o aplicativo exibirá um aviso indicando que essa configuração poderá causar uma falha no sistema.

- Foi adicionada a possibilidade de criar automaticamente as regras de permissão para o Controle de Inicialização de Aplicativos, além de exportar essas regras para um arquivo. Para fazer isso, execute a tarefa *Gerador de Regras de Controle de Inicialização de Aplicativos* e ative a criação automática de regras de permissão de acordo com os aplicativos em execução, assim como a exportação de regras de permissão. É possível usar o arquivo resultante para inventariar o software instalado no dispositivo.

- Novo componente, *Prevenção contra ataque BadUSB*. O componente Prevenção contra ataque BadUSB previne dispositivos de USB infectados que emulam um teclado de unir-se ao computador. Quando um dispositivo USB, identificado pelo sistema operacional como um teclado, é conectado ao computador, o aplicativo solicita que o usuário digite nesse teclado para autorizar o dispositivo.

- O *Indicador de nível de segurança* foi adicionado. O indicador de nível de segurança é exibido na parte superior da janela de propriedades da política e mostra o grau de conformidade das configurações de segurança com as recomendações da Kaspersky Lab. O indicador de nível de segurança permite configurar rapidamente a política e ativar os componentes de proteção necessários.

Kit de distribuição

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

- Inicie o Assistente de Instalação do Kaspersky Embedded Systems Security.
- Inicie o Assistente de Instalação do Console do Kaspersky Embedded Systems Security.
- Inicie a Ferramenta de Remoção de Vírus da Kaspersky .
- Leia sobre esta versão do Kaspersky Embedded Systems Security.
- Abra a Ajuda do Kaspersky Embedded Systems Security 4.0.
- Acesse a página do Kaspersky Embedded Systems Security no site da Kaspersky.
- Acesse o site da Kaspersky .
- Acesse o site de Suporte Técnico.

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

Arquivos do kit de instalação do Kaspersky Embedded Systems Security

Arquivo	Finalidade
autorun.inf	Arquivo de execução automática do Assistente de instalação do Kaspersky Embedded Systems Security para instalar o aplicativo de uma unidade removível.
setupui.exe	Arquivo de inicialização da tela de boas-vindas do aplicativo.

Arquivo	Finalidade
ess_win.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 de instalação do Windows Installer; instala o Kaspersky Embedded Systems Security Console nos dispositivos protegidos.
\console\setup_esstool.exe	Arquivo de inicialização para o assistente de instalação de um conjunto de componentes das Ferramentas de Administração (incluindo o Kaspersky Embedded Systems Security). O arquivo do pacote de instalação esstools.msi é iniciado com as configurações de instalação especificadas no assistente.
\console\license.txt	Arquivo de texto do Contrato de Licença do Usuário Final e da Política de Privacidade do Console de Gerenciamento do Kaspersky Embedded Systems Security.
\exec\bases.cab	Arquivo comprimido dos bancos de dados de antivírus na data de lançamento do aplicativo.
\exec\cleaner_v2.cab \exec\cleanerapi_v2.cab	Arquivos para remover o software incompatível.
\exec\ess.cab	Arquivos para a interface gráfica do aplicativo.
\exec\ess_win.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.
\exec\ess_win.msi	Pacote de instalação do Windows Installer: instala o Kaspersky Embedded Systems Security no dispositivo protegido.
\exec\incompatible.txt	A Kaspersky não garante a compatibilidade do Kaspersky Embedded Systems Security com os aplicativos listados no arquivo.
\exec\installer.ini	Arquivo que contém as configurações internas do kit de distribuição.
\exec\klcfginst.msi	Instalador do plug-in de administração do Kaspersky Embedded Systems Security disponível por meio do Kaspersky Security Center. Instale o Plug-in de Administração em cada dispositivo protegido em que o Console de Administração do Kaspersky Security Center estiver instalado caso pretenda usá-lo para gerenciar o Kaspersky Embedded Systems Security.
\exec\ksn_en.txt	Arquivo com o texto da Declaração da KSN.
\exec\license.txt	Arquivo de texto do Contrato de Licença do Usuário Final e da Política de Privacidade do Kaspersky Embedded Systems Security.
\exec\package.kcat	Arquivo com as assinaturas dos arquivos do kit de distribuição.
\exec\setup_ess.exe	O arquivo que inicia o assistente para a instalação do Kaspersky Embedded Systems Security no dispositivo protegido; ele inicia o arquivo do pacote de instalação ess_win.msi com as configurações de instalação especificadas no assistente.
\kvrt\KVRT.exe	Instalador da Ferramenta de Remoção de Vírus da Kaspersky .
\product_long_term\cleaner_v2.cab \product_long_term\cleanerapi_v2.cab	Arquivos para remover o software incompatível.
\product_long_term\ess.cab	Arquivos para a interface gráfica do aplicativo.
\product_long_term\ess_win.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.
\product_long_term\ess_win.msi	Pacote de instalação do Windows Installer; instala o Kaspersky Embedded Systems Security com a configuração **Proteja o computador com a tecnologia Default Deny** no dispositivo protegido.
\product_long_term\incompatible.txt	A Kaspersky não garante a compatibilidade do Kaspersky Embedded Systems Security com os aplicativos listados no arquivo.
\product_long_term\installer.ini	Arquivo que contém as configurações internas do kit de distribuição.
\product_long_term\klcfginst.exe	Instalador do plug-in de administração do Kaspersky Embedded Systems Security disponível por meio do Kaspersky Security Center. Instale o Plug-in de Administração em cada dispositivo protegido em que o Console de Administração do Kaspersky Security Center estiver instalado caso pretenda usá-lo para gerenciar o Kaspersky Embedded Systems Security.
\product_long_term\ksn_en.txt	Arquivo com o texto da Declaração da KSN em russo.
\product_long_term\license.txt	Arquivo de texto do Contrato de Licença do Usuário Final e da Política de Privacidade do Kaspersky Embedded Systems Security.
\product_long_term\package.kcat	Arquivo com as assinaturas dos arquivos do kit de distribuição.

Arquivo	Finalidade
\product_long_term\setup_ess.exe	O arquivo que inicia o assistente para a instalação do Kaspersky Embedded Systems Security no dispositivo protegido; ele inicia o arquivo do pacote de instalação ess_win.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 strings do aplicativo.

Os arquivos do kit de distribuição podem ser executados a partir do CD de instalação. Caso tenha copiado os arquivos do pacote de distribuição para a unidade local, assegure-se de que a estrutura dos arquivos do kit de distribuição tenha sido preservada.

Requisitos de hardware e software

Requisitos de software para o dispositivo protegido

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 nos dispositivos protegidos com sistemas operacionais incorporados, é necessário ter o componente (Filter Manager).

Para a operação correta do Kaspersky Embedded Systems Security, o suporte a SHA-2 no Microsoft Windows é necessário. Para obter informações detalhadas, consulte a base de conhecimento no site de Suporte Técnico.

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

Estações de trabalho:

- Windows XP Professional SP2 e posteriro 32 bits/64 bits
- Windows Vista SP2 32 bits/64 bits
- Windows 7 SP1 e posterior Home/Pro/Enterprise/Ultimate 32 bits/64 bits
- Windows 8 Pro/Enterprise 32 bits/64 bits
- Windows 8.1 Pro/Enterprise 32 bits/64 bits
- Windows 10 TH1 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 TH2 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits

- Windows 10 RS1 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 RS2 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 RS3 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 RS4 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 RS5 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 RS6 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 19H2 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 20H1 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 20H2 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 21H1 Home/Pro/Pro for Workstations/Education/Enterprise 32 bits/64 bits
- Windows 10 21H2 Home/Pro/Pro for Workstations/Education/Enterprise 64 bits
- Windows 10 22H2 Home/Pro/Pro for Workstations/Education/Enterprise 64 bits
- Windows 11 21H2 Home/Pro/Pro for Workstations/Education/Enterprise 64 bits
- Windows 11 22H2 Home/Pro/Pro for Workstations/Education/Enterprise 64 bits
- Windows 11 23H2 Home/Pro/Pro for Workstations/Education/Enterprise 64 bits
- Windows 11 24H2 Home/Pro/Pro for Workstations/Education/Enterprise 64 bits

Sistemas operacionais do servidor:

- Windows Server 2003 SP1 e posterior Standard/Enterprise 32 bits/64 bits
- Windows Server 2003 R2 SP2 Standard/Enterprise 64 bits
- Windows Server 2008 SP2 Standard/Enterprise 32 bits/64 bits
- Windows Server 2008 R2 SP2 e posterior Foundation/Standard/Enterprise 64 bits

Sistemas integrados:

- Windows XP Embedded SP3 POS Ready 32 bits
- Windows 7 Embedded POS Ready Standard 32 bits/64 bits
- Windows 7 Embedded SP1 Standard 32 bits/64 bits
- Windows 8.0 Embedded Standard 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 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
- Windows 11 versão 24H2 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	• 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
			• 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

Tipo de SO	Nome do SO	Requisitos mínimos	Requisitos recomendados

		• 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	

	Windows 7/8 Embedded
	Windows 10/11 IoT
		• Processador: processador de núcleo único de 1,4 GHz Pentium IV (x64).
		• RAM: 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

Versões compatíveis do Kaspersky Security Center

O Kaspersky Embedded Systems Security é compatível com as seguintes versões do Kaspersky Security Center:

- Kaspersky Security Center Windows versões 10.5, 11. O gerenciamento do Kaspersky Embedded Systems Security, instalado em computadores que executam o sistema operacional Microsoft Windows XP SP2, é compatível pelo Console de Administração do Kaspersky Security Center e Kaspersky Security Center Web Console.
- Kaspersky Security Center Windows versões 14.2, 15.1. Há suporte ao gerenciamento do Kaspersky Embedded Systems Security via Console de Administração do Kaspersky Security Center e Kaspersky Security Center Web Console.
- Kaspersky Security Center Linux versões 15.0, 15.1, 15.2, 15.3, 15.4 e 16.0. O gerenciamento do Kaspersky Embedded Systems Security é compatível pelo Kaspersky Security Center Web Console.

Para gerenciar o Kaspersky Embedded Systems Security pelo Kaspersky Security Center, é necessário ter o Agente de Rede do Kaspersky Security Center.

O Agente de Rede do Kaspersky Security Center não está incluído no kit de distribuição do Kaspersky Embedded Systems Security. É possível baixá-lo na página de download de aplicativos na seção **Kaspersky Security Center**.

Requisitos e limitações funcionais

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

Instalar e remover o aplicativo

- Para a operação correta do Kaspersky Embedded Systems Security, o suporte a SHA-2 no Microsoft Windows é necessário.

- Ao instalar o aplicativo, um aviso pode aparecer na tela se o caminho especificado para a pasta de instalação do Kaspersky Embedded Systems Security contiver mais de 150 caracteres. O aviso não afeta o processo de instalação: é possível instalar e executar o Kaspersky Embedded Systems Security.

- 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 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 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 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.

- Ao instalar o aplicativo em um dispositivo com Windows XP ou Windows Vista, talvez seja necessário instalar o certificado raiz DigiCert Assured ID Root CA para ativar a verificação de assinatura de drivers. Se necessário, esse certificado será instalado automaticamente no repositório de certificados raiz confiáveis do sistema operacional do pacote de instalação do aplicativo.

- Ao instalar o aplicativo em dispositivos com Windows XP ou Windows Vista, é necessário verificar se o certificado DigiCert High Assurance EV Root CA. está presente.

  Se esse certificado raiz não estiver instalado, o aplicativo poderá funcionar de forma incorreta. Recomendamos instalar o certificado o mais rápido possível.

- A instalação do aplicativo será concluída com um erro caso o caminho para a pasta de instalação seja o mesmo que o caminho para ao menos uma das seguintes pastas: pasta do bancos de dados do aplicativo, pasta de backup, pasta para a restauração de objetos da Quarentena, pasta de arquivos temporários.

- Caso gerencie o Kaspersky Embedded Systems Security usando o Kaspersky Security Center Cloud Console, a atualização local do aplicativo não será permitida. Ao atualizar o aplicativo localmente, não é possível aceitar o Contrato de Processamento de Dados para o Kaspersky Security Center Cloud Console.

Monitor de integridade do sistema

Por padrão, o componente Monitor de integridade do sistema 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).

Firewall

- É possível especificar mais de um endereço. Caso contrário, o trabalho com IPv6 estará indisponível.
- As regras 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 a configuração das regras do Firewall, o aplicativo monitora as alterações nas regras e nos grupos de regras do Firewall do Windows quando o Firewall está em execução. Para atualizar o status e adicionar as regras necessárias do Firewall do Windows, reinicie o componente Firewall.
- Ao iniciar o componente Firewall, as regras de negação e as regras que controlam o tráfego de saída são automaticamente removidas das configurações do Firewall do Windows.
- Os caracteres `*` e `?` não podem ser usados no caminho do aplicativo nem no nome da regra de Firewall para aplicativos.
- No sistema operacional Windows, nas configurações do Firewall (**Configurações → Atualização e segurança → Segurança do Windows → Firewall e proteção de rede**), o botão que ativa o Firewall do Kaspersky Embedded Systems Security ativa somente o Firewall, mas não o muda para o modo *Bloquear*, a menos que, antes de ativar o Firewall, estivesse ativado o modo *Observar o estado do Firewall do Windows*. Ao ativar o Firewall do Kaspersky Embedded Systems Security, o botão deixará de ser exibido somente depois que o modo do Firewall for alterado para *Bloquear*.

Limitações em versões desatualizadas do Windows

- A versão do Windows XP SP2 não permite bloquear dispositivos remotos e definir as configurações da lista de Sessões de rede bloqueadas. Nesta versão do Windows, a opção **Bloquear acesso a recursos compartilhados de rede para sessões que mostram atividade maliciosa** está inativa.
- Instalação do Kaspersky Embedded Systems Security:
  - Em computadores que executam Windows XP SP2 Professional (32 bits/64 bits), Windows Server 2003 e Windows Server 2003 R2, é necessário usar o kit de distribuição do aplicativo ou mover o arquivo executável setup.exe do pacote de instalação padrão "Agente de Rede para Windows XP do Kaspersky Security Center 10.5" para a pasta do pacote de instalação do aplicativo no Kaspersky Security Center .
  - Em computadores que executam Windows XP SP3 Professional (32 bits) e Windows XP Embedded SP3 (32 bits), é necessário usar o kit de distribuição do aplicativo ou mover o arquivo executável setup.exe do pacote de instalação do aplicativo criado no Kaspersky Security Center versão 14 ou do pacote de instalação padrão "Agente de Rede para Windows XP do Kaspersky Security Center 14" para a pasta do pacote de instalação do aplicativo no Kaspersky Security Center.

Como extrair o arquivo setup.exe do pacote de instalação padrão do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione **Avançado** → **Instalação remota** → **Pacotes de instalação**.
2. Na área de trabalho, clique em **Ações adicionais** e selecione **Exibir as versões atuais dos aplicativos da Kaspersky** na lista suspensa.
3. Selecione o aplicativo desejado na lista. Por exemplo, o Agente de Rede do Kaspersky Security Center 10.5 para Windows XP.
4. Clique no botão **Baixar e criar pacote de instalação**.

   O pacote de instalação criado será exibido na lista **Pacotes de instalação**.
5. Abra as propriedades do pacote de instalação criado.
6. Na seção **Geral**, copie o caminho para a pasta do pacote de instalação.
7. Abra a pasta do pacote de instalação.
8. Copie o arquivo setup.exe.

- Para gerenciar o Kaspersky Embedded Systems Security por meio do 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.
- Em computadores com Windows XP, a telemetria não pode ser enviada para um diodo de dados usando o protocolo MQTT.

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 do Kaspersky Security Center não verifica as atualizações dos módulos do aplicativo.
- Tenha certeza de que as caixas de seleção necessárias estejam marcadas nas configurações de Interação com o Servidor de Administração do Kaspersky Security Center ao usar os componentes que transmitem dados dinâmicos ao Kaspersky Security Center usando listas de rede (Quarentena, Backup).
- O Agente de Rede 10.5 não envia informações sobre os componentes instalados no Servidor de Administração do Kaspersky Security Center. Por esse motivo, no Console de Administração do Kaspersky Security Center e Kaspersky Security Center Web Console, as configurações de um dispositivo com o Agente de Rede 10.5 não exibem os componentes instalados do Kaspersky Embedded Systems Security e suas configurações.
- Caso o Agente de Rede 10.5 do Kaspersky Security Center esteja instalado no dispositivo, não será possível usar o Kaspersky Security Center Web Console para baixar arquivos do Backup.

- Caso o Kaspersky Embedded Systems Security seja instalado com o modo de consumo de baixo recurso ativado para o Agente de Rede do Kaspersky Security Center (padrão, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`), e em seguida, o Agente de Rede seja instalado, o Kaspersky Embedded Systems Security não criará uma exclusão para o Agente de Rede no Windows Firewall. Devido a isso, o Windows Firewall bloqueará o Agente de Rede.

- Caso o Kaspersky Embedded Systems Security seja instalado com o modo de consumo de baixo recurso ativado para o Agente de Rede do Kaspersky Security Center (padrão, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`), as modificações das listas de rede serão refletidas no Console de Administração do Kaspersky Security Center com um atraso aproximado de 10 minutos.

Outras limitações

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, 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 durante a análise)** e **Uso da KSN** sejam ativadas simultaneamente, qualquer processo iniciado que receba a URL do endereço da Web como argumento será bloqueado, mesmo que o modo "Informar" tenha sido escolhido. Para evitar o bloqueio do processo, escolha uma das opções:

  - Desativar o **Uso da KSN**.

  - Desmarcar a caixa de seleção **Análise profunda de processos sendo inicializados (a inicialização do processo é bloqueada durante a análise)**

  Opção recomendada: desmarque a caixa de seleção **Análise profunda de processos sendo inicializados (a inicialização do processo é bloqueada durante a análise)**.

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 são instaladas.
- KLRAMDISK não é compatível em dispositivos protegidos executando o sistema operacional Windows XP ou Windows Server® 2003.
- Caso a instalação do patch do Kaspersky Embedded Systems Security falhe, o patch será revertido e uma solicitação aparecerá para reiniciar o sistema operacional.

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 alguns exemplos de máscaras corretas: `C:\Temp\Temp*`, `C:\Temp\Temp???.doc`, `C:\Temp\Temp*.doc`. Essa limitação não afeta a configuração da Zona Confiável.
- No Console do Aplicativo, na seção **Servidores de coleta de telemetria**, a hora em que as tarefas estão agendadas para execução não é exibida. A coluna **Hora de início** está vazia.

Segurança

- Se o recurso de Controle de Conta de Usuário do sistema operacional for ativado, a conta de usuário deve fazer parte do grupo Administradores do ESS para ser possível abrir o Console do Aplicativo clicando duas vezes no ícone do aplicativo na área de notificação da bandeja. 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.

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 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 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.

Detection and Response

- Se ocorrer um erro de acesso à pasta compartilhada durante o processo de resposta a ameaças, ele não refletirá no histórico de resposta a ameaças (seção Kaspersky Security Center Web Console → propriedades do host com o aplicativo instalado → **Detection and Response** – **Histórico de resposta**).

- Não há suporte para a configuração [KESS+KEA+agente integrado]. Essa configuração interrompe a interação entre os aplicativos e a solução de Detection and Response em sua organização. Além disso, usar o Kaspersky Endpoint Agent e o agente integrado no mesmo computador pode levar à duplicação da telemetria e aumentar a carga no computador e na rede.

  O instalador permite implementar o Kaspersky Endpoint Agent em um computador com o Kaspersky Embedded Systems Security e o agente integrado instalado. O Kaspersky Endpoint Agent e o agente integrado também podem ser instalados em um computador como resultado da tarefa *Alterar componentes do aplicativo*. O comportamento depende das versões do Kaspersky Embedded Systems Security e do Kaspersky Endpoint Agent.

Configuração de eventos

As configurações do evento *Operação suspeita com arquivos em área controlada* que podem ser configuradas na seção **Configuração de eventos** da política do Kaspersky Security Center, também são aplicadas aos seguintes eventos:

- *Operação de arquivo permitida em uma área controlada realizada por um usuário confiável*.
- *Prohibited file operation in controlled area*.
- *Somente para estatística: operação de arquivo proibida em área controlada*.
- *Operação de arquivo não controlado na área controlada*.

Interface de diagnóstico compacta

Em computadores com Windows XP, a Interface de diagnóstico compacta requer que o Serviço de terminal esteja em funcionamento.

Compatibilidade com outros aplicativos

O Kaspersky Embedded Systems Security na configuração de *Funcionalidade completa* é incompatível com aplicativos que fazem parte de sistemas de proteção de endpoint de terceiros (Endpoint Protection Platform, EPP). O Kaspersky Embedded Systems Security também pode ser incompatível com aplicativos de outros fornecedores e alguns aplicativos da Kaspersky. Para determinar a compatibilidade, o Kaspersky Embedded Systems Security consulta uma lista de softwares preparada pela Kaspersky. Essa lista está contida no arquivo incompatible.txt. O arquivo está incluído no kit de distribuição.

Se um aplicativo da lista incompatible.txt for detectado, o instalador interromperá a instalação do Kaspersky Embedded Systems Security. É necessário remover o aplicativo antivírus de terceiros. O instalador pode excluir automaticamente alguns aplicativos da lista.

Se o Firewall do Windows estiver instalado no computador, o instalador o desativará para prosseguir com a instalação do Kaspersky Embedded Systems Security.

Se, apesar dos riscos, for necessário instalar o Kaspersky Embedded Systems Security junto com um aplicativo da lista incompatible.txt, será possível ignorar a verificação de aplicativos antivírus de terceiros instalados. Para isso, passe o parâmetro `SKIPINCOMPATIBLESW= 1` para o instalador.

Exemplo:

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 /p  SKIPINCOMPATIBLESW= 1
```

Instalar e remover o aplicativo

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

Planejamento da instalação

Esta seção descreve o conjunto de ferramentas de administração do Kaspersky Embedded Systems Security e os aspectos especiais da instalação e desinstalação do Kaspersky Embedded Systems Security usando um assistente, a linha de comando, o Kaspersky Security Center e uma política de grupo do Active Directory.

Caso esteja instalando o Kaspersky Embedded Systems Security após remover o Kaspersky Industrial CyberSecurity for Nodes ou o Kaspersky Endpoint Security for Windows, reinicie o computador.

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

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

O Console do Kaspersky Embedded Systems Security é um snap-in independente adicionado ao Console de Gerenciamento da Microsoft. O Kaspersky Embedded Systems Security 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 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 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 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.

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 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. Ele permite a comunicação do Kaspersky Embedded Systems Security 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 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 Gerenciamento do Kaspersky Embedded Systems Security**. Adicionalmente, instale o plug-in de administração para gerenciar o Kaspersky Embedded Systems Security por meio do Console de Administração no dispositivo protegido no qual o 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.

Seleção do tipo de instalação

Depois de especificar os componentes do software para instalação do Kaspersky Embedded Systems Security, 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 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 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 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 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 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 no dispositivo protegido ao clicar no link no aplicativo de boas-vindas, que pode ser iniciado ao abrir o setupui.exe, ou ao usar diretamente o arquivo \exec\setup_ess.exe no kit de distribuição.

- O Console do Kaspersky Embedded Systems Security no dispositivo protegido ou em outro dispositivo na rede local clicando no link no aplicativo de boas-vindas, que pode ser iniciado abrindo o setupui.exe ou usando diretamente o arquivo \console\setup_esstools.exe no kit de distribuição.

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 será instalado com a configuração padrão. As opções especiais do Kaspersky Embedded Systems Security 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 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 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 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 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 pode ser instalado usando somente as configurações de instalação recomendadas.

Os dispositivos protegidos nos quais o Kaspersky Embedded Systems Security 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 e do Console do Aplicativo por meio do assistente de instalação e contém informações sobre as configurações adicionais do Kaspersky Embedded Systems Security 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 e do Console do Aplicativo.

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

1. Instale o Kaspersky Embedded Systems Security no dispositivo protegido.
2. Instale o Console do Aplicativo nos dispositivos a partir dos quais pretende gerenciar o Kaspersky Embedded Systems Security.
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.
4. Realize ações após a instalação do Kaspersky Embedded Systems Security.

Instalação do Kaspersky Embedded Systems Security

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

1. Certifique-se de que nenhum outro programa antivírus esteja instalado no dispositivo protegido. É necessário remover o Kaspersky Anti-Virus 8.0 for Windows Server Enterprise Edition. Não é necessário remover o Kaspersky Security 10 for Windows Server para instalar o Kaspersky Embedded Systems Security.
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 de acordo com as instruções do Assistente de instalação. O processo de instalação do Kaspersky Embedded Systems Security 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 usando o assistente de instalação:

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

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

   Caso a configuração **Proteger o computador com bases de antivírus"** seja selecionada, todos os componentes do Kaspersky Embedded Systems Security serão incluídos por padrão, exceto os componentes 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 as 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"** for selecionada, os seguintes componentes serão incluídos por padrão:

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

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

   - Proteção de Arquivos em Tempo Real
   - Verificação por demanda.
   - os componentes que possibilitam 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, clique no botão **Avançar >**.

   A janela **Contrato de Licença do Usuário Final** é aberta.

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 a Política de Privacidade, marque as caixas de seleção **Confirmo que li, entendi e concordo integralmente com os termos e condições desses Contratos de licença do usuário final** e **Estou ciente e concordo que meus dados serão manuseados e transmitidos (inclusive para outros países) conforme descrito na Política de privacidade. Eu li, entendi e concordo completamente com a Política de privacidade**.

   Se você não aceitar o Contrato de Licença do Usuário Final e/ou a Política de Privacidade, a instalação será interrompida.

6. Clique **Avançar >**.

   A janela **Instalação personalizada** é aberta.

7. Selecione os componentes a serem instalados.

   O componente de suporte do protocolo SNMP do Kaspersky Embedded Systems Security 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 **Reiniciar** na janela **Instalação personalizada**. Clique **Avançar >**.

9. Na janela **Selecione a pasta de destino**, faça o seguinte:

   - Se necessitado, especifique uma pasta à qual os arquivos do Kaspersky Embedded Systems Security serão copiados.
   - Se necessário, leia as informações sobre o espaço disponível nas unidades locais clicando no botão **Disco**.

   Clique **Avançar >**.

10. Na janela **Configurar**, é possível excluir objetos e pastas do escopo de proteção e configurar a Proteção de Arquivos em Tempo Real.

11. Na janela **Importar configurações do arquivo de configuração**, especifique um caminho para o arquivo de configuração, caso queira importar as configurações do Kaspersky Embedded Systems Security de um arquivo de configuração existente criado em um versão anterior do aplicativo.

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 para a ativação do aplicativo.
    - Caso queira ativar o aplicativo mais tarde, clique no 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.

O assistente de instalação não permite ativar o aplicativo com um código de ativação. Caso queira ativar o aplicativo com um código de ativação, será possível especificar um código após a instalação.

Após o arquivo de chave ser adicionado, as informações da licença serão mostradas na janela. O Kaspersky Embedded Systems Security 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 em **Avançar >** para adicionar o arquivo de chave para o aplicativo.

13. Na seção **Configurações de acesso remoto**, se necessário, altere os números da porta TCP usados pelo Console do Aplicativo para conexão remota ao computador com o aplicativo instalado.

    O número da porta padrão para conexão com credenciais do Windows é 13032 e o número da porta padrão para conexão com credenciais de usuários criados manualmente é 13031. Intervalo de números de porta possíveis: 1 a 65535.

    Para impedir a conexão com credenciais de contas de usuário criadas manualmente, desmarque a caixa de seleção **Uso das credenciais de usuários criados manualmente**.

14. Na janela **Pronto para instalar**, é possível desativar a opção **Proteger o processo de instalação do aplicativo**, se necessário. A proteção da instalação inclui proteção contra a substituição do pacote de distribuição por aplicativos maliciosos, bloqueio do acesso à pasta de instalação do Kaspersky Embedded Systems Security e bloqueio do acesso à seção de registro do sistema que contém chaves do aplicativo. Caso não seja possível instalar o aplicativo (por exemplo, ao efetuar a instalação remota com ajuda do Windows Remote Desktop), é aconselhável desativar a proteção do processo de instalação.

15. Se necessário, adicione o caminho do arquivo kavshell.exe na variável de sistema %PATH% para uso da interface da linha de comando.

16. Clique **Instalar**.

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

18. Clique no botão **Concluir**.

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

Instalação do Console do Kaspersky Embedded Systems Security

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. Clique **Avançar >**.

4. Caso concorde com os termos e condições do Contrato de Licença do Usuário Final e a Política de Privacidade, marque as caixas de seleção **Confirmo que li, entendi e concordo integralmente com os termos e condições desses Contratos de licença do usuário final** e **Estou ciente e concordo que meus dados serão manuseados e transmitidos (inclusive para outros países) conforme descrito na Política de privacidade. Eu li, entendi e concordo completamente com a Política de privacidade**. Clique **Avançar >**.

5. Especifique uma pasta na qual os arquivos que estão sendo instalados devem ser salvos na janela **Selecione a pasta de destino**.

6. Clique **Avançar >**.

7. Clique no botão **Instalar** na subseção **Pronto para instalar**.

   O assistente começará a instalação dos componentes selecionados.

8. Clique **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 remotamente:

- Use uma conta de usuário com permissão para se conectar remotamente nas configurações do aplicativo. Por padrão, todos os usuários nos grupos Administradores e Administradores de ESS têm essa permissão.

- No dispositivo remoto, nas configurações do Firewall do Windows, abra a porta TCP 13032 para conexão por contas de usuário do sistema Windows e TCP 13031 para conexão por contas de usuário criadas manualmente nas configurações do aplicativo. Permita também as conexões de rede para o arquivo executável do processo de gerenciamento remoto do Kaspersky Embedded Systems Security, avp.exe. É possível gerenciar essa configuração usando a opção `ADDWFEXCLUSION=1` ao instalar o aplicativo na linha de comando.

Caso precise executar o Kaspersky Embedded Systems Security remotamente, faça o seguinte:

A conta de usuário que iniciará remotamente o aplicativo deve fazer parte do grupo Administradores.

- No dispositivo remoto, nas configurações do Firewall do Windows, ative a regra **Compartilhamento de arquivos e impressoras (SMB-In)** (porta TCP 445). Além disso, recomendamos abrir a porta TCP 135 para facilitar a conexão com o dispositivo.

- Para os dispositivos remotos que executam o Windows Vista ou posterior, e que não fazem parte de um domínio ou são gerenciados por uma conta de usuário local, **desative o controle remoto de contas de usuário (UAC).**

  1. Abra o editor de registro no computador.
  2. No editor de registro, abra a chave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.
  3. Abra o valor LocalAccountTokenFilterPolicy.

     Caso o valor LocalAccountTokenFilterPolicy esteja ausente nessa chave, crie um valor DWORD (32 bits) com esse nome (para obter detalhes, consulte o site de Suporte Técnico da Microsoft).
  4. Defina-o como `1` e clique em **OK**.

     A desativação do UAC remoto não afeta o UAC local.

- Caso o dispositivo no qual o Console do Aplicativo esteja instalado ou o dispositivo protegido execute o Windows 8.1 ou uma versão anterior do Windows, **ative o suporte ao acesso compartilhado a arquivos SMB 1.0/CIFS em dispositivos que executem o Windows 10 ou versões posteriores.**

  - No aplicativo "Recursos do Windows":
    1. Selecione **Iniciar** → **Painel de Controle** → **Programas e recursos** → **Ativar ou desativar os recursos do Windows**.
    2. Na janela **Recursos do Windows**, marque a caixa de seleção **Suporte ao compartilhamento de arquivos SMB 1.0/CIFS**.
    3. Clique em **OK**.
  - No Windows PowerShell:
    1. Execute o Windows PowerShell como administrador.
    2. Execute o seguinte comando:

       ```
       Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
       ```

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 avp.exe seja concluído.
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 instalado, abra o console de **Serviços do componente**. Para fazer isso:
   a. Selecione **Iniciar** → **Executar**.
   b. Execute o comando `dcomcnfg`.
   c. O console **Serviços do componente** é aberto.
2. Expanda o node **Computadores** no console de **Serviços do componente** em seu dispositivo protegido.
3. Abra o menu de contexto no node **Meu computador**.
4. Selecione **Propriedades**.
5. Na guia **Segurança COM** da janela **Propriedades**, clique no botão **Editar limites** no grupo de configurações **Permissões de acesso**.
6. Certifique-se de que a caixa de seleção **Permitir Acesso Remoto** esteja marcada para o usuário ANONYMOUS LOGON na janela **Permitir Acesso Remoto**.
7. Clique em **OK**.

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

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:

1. Feche o Console do Kaspersky Embedded Systems Security 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 DCOM, e especifique o número da porta (135) no campo **Nome da porta**.
     d. Selecione o protocolo **TCP**.
     e. Clique em **OK**.
     f. Clique no botão **Adicionar** na guia **Exclusões**.
   - No Microsoft Windows 7 ou 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 aplicativo**. Ele está localizado na pasta especificada como pasta de destino durante a instalação do Console do Kaspersky Embedded Systems Security usando o Console de Gerenciamento Microsoft.
4. Clique em **OK**.
5. Clique no botão **OK** na janela **Firewall do Windows (Configurações do Firewall do Windows)**.

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

O Kaspersky Embedded Systems Security iniciará as tarefas de proteção e verificação imediatamente após a instalação se o aplicativo tiver sido ativado. Caso a caixa de seleção **Ativar a Proteção de Arquivos em Tempo Real após a instalação do aplicativo (recomendado)** tenha sido selecionada durante a instalação do Kaspersky Embedded Systems Security, o aplicativo verificará os objetos do sistema de arquivos do dispositivo quando eles forem acessados. Caso o componente de monitoramento de scripts tenha sido instalado como parte da instalação personalizada, o Kaspersky Embedded Systems Security verificará o código fonte de todos os scripts quando eles forem iniciados. O Kaspersky Embedded Systems Security 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:

- Inicie a tarefa Atualização do Banco de Dados do aplicativo. Após a instalação, o Kaspersky Embedded Systems Security 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 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.

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

Inicialização e configuração da tarefa de atualização de bancos de dados e módulos do aplicativo

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

1. Na tarefa de atualização de bancos de dados e módulos do aplicativo, configure a conexão para a fonte de atualização.
2. Inicie a tarefa de atualização de bancos de dados e módulos do aplicativo.

O Web Proxy Auto-Discovery Protocol (WPAD) talvez não esteja configurado na sua rede para detectar automaticamente as configurações do servidor proxy 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 nó **Kaspersky Embedded Systems Security**.
2. Selecione **Propriedades do aplicativo**.
3. Na janela que é aberta, selecione a guia **Configurações de rede**.
4. Na seção **Configurações do servidor proxy**, clique em **Configurações**, e na janela exibida, 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:

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

   - **Autenticação NTLM com nome de usuário e senha** se o servidor proxy suportar a autenticação NTLM integrada do Microsoft Windows. O Kaspersky Embedded Systems Security usará a conta especificada para acessar o servidor proxy. Insira um nome de usuário e a senha ou selecione um usuário na lista.

   - **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**.

Para executar a tarefa de atualização de bancos de dados e módulos do aplicativo:

1. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.

2. No menu de contexto do nó secundário **Atualização do banco de dados**, selecione o item **Iniciar**.

   A tarefa de atualização de bancos de dados e módulos do aplicativo 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**.

Verificação de Áreas Críticas

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

Para executar a tarefa Verificação de áreas críticas:

1. Na árvore do Console do Aplicativo, expanda o nó **Verificação por demanda**.

2. No menu de contexto do nó secundário **Verificação de áreas críticas**, selecione o comando **Iniciar**.

A tarefa inicia; o status **Em execução** 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

Os componentes do Kaspersky Embedded Systems Security 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 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:

1. No Windows **Painel de Controle**, selecione **Aplicativos e recursos**. A janela **Modificar ou Remover** do assistente é exibida.
2. Clique com o botão direto em **Kaspersky Embedded Systems Security** e selecione **Editar**.

   Esse procedimento abrirá o assistente de configuração **Modificar, reparar ou remover o aplicativo**.
3. Selecione **Modificar**.

   A janela **Instalação personalizada** é aberta. Selecione **Funcionalidade completa** e clique em **Avançar >**.
4. Na janela **Instalação personalizada**, na lista de componentes disponíveis, selecione os componentes que deseja adicionar ao Kaspersky Embedded Systems Security 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 recurso será instalado no disco rígido local**, caso queira instalar um componente;
     - **Todo o recurso e seus sub-recursos serão instalados no disco rígido local**, caso queira 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 recurso não estará disponível**.

   Clique **Avançar >**.
5. Na janela **Pronto para instalar**, confirme a seleção dos componentes do aplicativo ao clicar em **Instalar**.
6. Na janela aberta quando a instalação for concluída, clique no botão **Concluir**.

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

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

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

1. No Windows **Painel de Controle**, selecione **Aplicativos e recursos**. A janela **Modificar ou Remover** do assistente é exibida.
2. Clique com o botão direto em **Kaspersky Embedded Systems Security** e selecione **Editar**.
3. Esse procedimento abrirá o assistente de configuração **Modificar, reparar ou remover o aplicativo**.
4. Selecione a opção **Reparar**.

   A janela **Reparar o Kaspersky Embedded Systems Security** é aberta. Clique **Avançar >**.
5. Aguarde até que a operação de restauração seja concluída e, na janela exibida, clique em **Concluir**.

O Kaspersky Embedded Systems Security 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 e do Console do Aplicativo de um dispositivo protegido usando o Assistente de instalação/desinstalação.

Desinstalação do Kaspersky Embedded Systems Security

Os arquivos de despejo e rastreamento não são excluídos na desinstalação do Kaspersky Embedded Systems Security. 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 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 de um dispositivo protegido. A reinicialização pode ser adiada.

A desinstalação, o reparo e a instalação do aplicativo não estão disponíveis via Painel de Controle do Windows.

O Kaspersky Embedded Systems Security solicita as credenciais da conta do usuário quando o usuário tenta remover ou modificar o conjunto de componentes no Assistente de Instalação. Você precisa inserir as credenciais de um usuário com direitos suficientes. Se uma senha vazia do Windows estiver definida para a conta de usuário que realizará a remoção, desative a funcionalidade **Solicitar senha para confirmar ações críticas** antes de iniciar a remoção.

Para desinstalar o Kaspersky Embedded Systems Security:

1. No Windows **Painel de Controle**, selecione **Aplicativos e recursos**. A janela **Modificar ou Remover** do assistente é exibida.
2. Clique com o botão direto em **Kaspersky Embedded Systems Security** e selecione **Editar**.
3. Esse procedimento abrirá o assistente de configuração **Modificar, reparar ou remover o aplicativo**.
4. Selecione **Remover**.

   A janela **Salvar objetos** é aberta.
5. Caso seja necessário, na janela **Salvar objetos**, faça o seguinte:

   Em **Salvar objetos**, especifique quais são os objetos ou configurações que se deseja manter. Por padrão, a caixa de seleção fica desmarcada.

   - Marque a caixa de seleção **Dados de ativação**.
   - Marque a caixa de seleção **Arquivos de Backup**.
   - Marque a caixa de seleção **Configurações operacionais do aplicativo**.

   Em **Exportar objetos**, especifique quais são os objetos ou configurações que deseja exportar. Por padrão, a caixa de seleção fica desmarcada.

   - Marque a caixa de seleção **Exportar objetos da quarentena** para que o Kaspersky Embedded Systems Security exporte objetos que foram colocados em quarentena. Por padrão, a caixa de seleção fica desmarcada.
   - Marque a caixa de seleção **Exportar objetos do backup** para exportá-los a partir do Backup do Kaspersky Embedded Systems Security. Por padrão, a caixa de seleção fica desmarcada.
   - Clique no botão **Salvar** e selecione a pasta para onde deseja exportar os objetos. Por padrão, os objetos serão exportados para %ProgramData%\Kaspersky Lab\KESS.4.0\QB.

     Clique **Avançar**.
6. Na janela **Pronto para desinstalar**, confirme a remoção clicando em **Remover**.
7. Na janela exibida quando a desinstalação for concluída, clique no botão **Concluir**.

O Kaspersky Embedded Systems Security será desinstalado do dispositivo protegido.

Desinstalação do Console do Kaspersky Embedded Systems Security

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 Windows **Painel de Controle**, selecione **Aplicativos e recursos**. A janela **Modificar ou Remover** do assistente é exibida.
2. Clique com o botão direto em **Kaspersky Embedded Systems Security Console** e selecione **Editar**.

   A janela **Modificar, reparar ou remover o aplicativo** do assistente será aberta.
3. Selecione **Remover**.

   A janela **Pronto para desinstalar** é aberta. Clique **Desinstalar**.
4. Na janela exibida quando a desinstalação for concluída, 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 na linha de comando e contém exemplos de comandos para instalar e desinstalar o Kaspersky Embedded Systems Security na linha de comando e exemplos de comandos para adicionar e remover os componentes do Kaspersky Embedded Systems Security na linha de comando.

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

Os arquivos de despejo e rastreamento não são excluídos na desinstalação do Kaspersky Embedded Systems Security. 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 e adicionar ou remover seus componentes ao executar o arquivo do pacote de instalação \exec\ess_win.msi a partir da linha de comando após especificar as configurações de instalação com o uso das 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 o arquivo \exec\ess_win.msi seja executado no dispositivo protegido sem opções adicionais na linha de comando, o Kaspersky Embedded Systems Security 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.

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

O arquivo \product_long_term\ess_win.msi é projetado para instalar a configuração **Proteger o computador com tecnologia de Negação padrão** do Kaspersky Embedded Systems Security, e o arquivo \exec\ess_win.msi é projetado para instalar a configuração **Proteger o computador com bases de antivírus** do Kaspersky Embedded Systems Security.

Caso a configuração **Proteger o computador com bases de antivírus"** seja selecionada, todos os componentes do Kaspersky Embedded Systems Security serão incluídos por padrão, exceto os componentes 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 as 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"** for selecionada, os seguintes componentes serão incluídos por padrão:

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

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

- Proteção de Arquivos em Tempo Real
- Verificação por demanda.
- os componentes que possibilitam 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.

O arquivo \console\esstools.msi instala 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 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 na linha de comando.

Componentes de software do Kaspersky Embedded Systems Security

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

Descrição dos componentes de software do Kaspersky Embedded Systems Security

Componente	Código	Funções do componente
Proteção de Arquivos em Tempo Real	`FileThreatProtection`	Esse componente executa verificações de vírus de arquivos no dispositivo protegido quando esses arquivos são acessados.
Scanner AMSI	`AMSI`	O componente tem o objetivo de oferecer suporte à Antimalware Scan Interface da Microsoft. A Antimalware Scan Interface (AMSI) permite que aplicativos de terceiros com suporte a AMSI envie objetos (por exemplo, scripts do PowerShell) para o Kaspersky Embedded Systems Security para uma verificação adicional e receber os resultados da verificação desses objetos.
Detecção de Comportamento	`BehaviorDetection`	Esse componente preenche a lista de hosts bloqueados com os nomes dos dispositivos remotos que apresentam atividade maliciosa.
Prevenção de Exploit	`ExploitPrevention`	Esse componente permite gerenciar as configurações para proteger a memória usada por processos na memória de um dispositivo.
Mecanismo de Remediação	`RemediationEngine`	O componente permite que o Kaspersky Embedded Systems Security desfaça ações executadas por malware no sistema operacional.
Firewall	`Firewall`	Esse componente permite gerenciar o firewall do Windows por meio da interface gráfica do usuário do Kaspersky Embedded Systems Security.
Proteção Contra Ameaças à Rede	`NetworkThreatProtection`	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 bloqueará a atividade de rede do computador invasor.
Controle de Inicialização de Aplicativos	`ApplicationControl`	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.
Controle de Dispositivos	`DeviceControl`	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.

Componente	Código	Funções do componente
Módulo para integração com o Agente de Rede do Kaspersky Security Center.	`AdminKitConnector`	Fornece uma conexão entre o Kaspersky Embedded Systems Security e o Agente de Rede do Kaspersky 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.
Monitor de integridade do sistema	`SystemIntegrityMonitor`	O componente inclui todas as funcionalidades do Monitor de Integridade de Arquivos. Além disso, ele permite monitorar as alterações do registro e a conexão de dispositivos externos.
Prevenção contra ataque BadUSB	`BadUSBAttackPrevention`	O componente impede que dispositivos USB infectados e que emulam um teclado se conectem ao computador.
Managed Detection and Response	`MDR`	Esse componente facilita a interação com a solução Kaspersky Managed Detection and Response.

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	MmcSnapin	Esse componente instala o snap-in do Console de Gerenciamento Microsoft por meio do Console do Kaspersky Embedded Systems Security. O MmcSnapin é instalado automaticamente; ele não precisa ser especificado nos parâmetros do comando de instalação.

Configurações de instalação e recuperação e opções de linha de comando do Windows Installer

Esta seção detalha as configurações de instalação e recuperação do Kaspersky Embedded Systems Security . A seção também contém as chaves para alterar as configurações de instalação e possíveis valores de chave. 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 a partir da linha de comando.

Configurações de instalação e opções de linha de comando do Windows Installer

- Aceitação dos termos do Contrato de Licença do Usuário Final.

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

  - `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.

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

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

- Instalação do Kaspersky Embedded Systems Security 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 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).

- Pasta de destino onde os arquivos do Kaspersky Embedded Systems Security 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:

  - Para a versão de 32 bits do Microsoft Windows:

    - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0

    - Kaspersky Embedded Systems Security Console: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools.4.0.0

  - Para a versão de 64 bits do Microsoft Windows: %ProgramFiles(x86)% e além, semelhante aos caminhos das versões de 32 bits do Microsoft Windows.

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

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

  - `1` – iniciar (valor padrão).

  - `0` – não iniciar.

- 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 em outro caminho a ser especificado no parâmetro `LICENSEKEYPATH`.

`LICENSEKEYPATH` pode ter os seguintes valores.

- Caminho completo para o arquivo de chave incluindo o nome do arquivo.
- Caminho para a pasta onde os arquivos de chave estão armazenados.

É possível adicionar uma chave depois que o Kaspersky Embedded Systems Security 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 não funcionará.

- Caminho do arquivo de configuração. O Kaspersky Embedded Systems Security importa configurações do arquivo de configuração especificado criado no aplicativo. O Kaspersky Embedded Systems Security 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 *Verificação na Inicialização do Sistema Operacional* (SCANSTARTUP_BLOCKING). Caso o Kaspersky Embedded Systems Security tenha sido instalado sem uma chave SCANSTARTUP_BLOCKING, o parâmetro **Escopo da verificação** na tarefa *Verificação na Inicialização do Sistema Operacional* será definido da seguinte forma:

  - Ação a ser executada em objetos infectados e outros: **Informar**.
  - Ação a ser executada em objetos possivelmente infectados: **Informar**.

  Caso o Kaspersky Embedded Systems Security tenha sido instalado com uma chave SCANSTARTUP_BLOCKING, o parâmetro **Escopo da verificação** na tarefa *Verificação na Inicialização do Sistema Operacional* será definido da seguinte forma:

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

  A tarefa *Verificação na Inicialização do Sistema Operacional* é criada automaticamente. O modo **Informar** é aplicado por padrão. Nesse caso, depois de implementar o Kaspersky Embedded Systems Security nos dispositivos, será possível ativar a tarefa de *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 **Informar** dará tempo para descobrir o motivo e resolver o problema. Caso o aplicativo aplique o modo **Executar ação recomendada**, a ação **Desinfectar e excluir se a desinfecção falhar** será executada. A desinfecção ou remoção dos arquivos do sistema pode resultar em problemas críticos com a inicialização do sistema operacional.

- 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, 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:

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

- Desativação da verificação para a atualização do sistema operacional KB5007186.

  Após instalar a atualização KB5007186, o aplicativo continuará funcionando normalmente, a segurança do sistema não será comprometida, mas pequenas atualizações de versões dos aplicativos serão impossíveis. Antes de instalar o aplicativo, o instalador verificará as atualizações já instaladas no sistema operacional. Caso a atualização KB5007186 seja descoberta, o instalador abortará a instalação. É possível usar a chave `SKIPKB5007186CHECK` na linha de comando para ativar ou desativar a verificação para a atualização do sistema operacional KB5007186.

  Os valores possíveis para a opção `SKIPKB5007186CHECK=<valor>` na linha de comando são:

  - `0`: O instalador verifica se a atualização do sistema operacional KB5007186 está instalada.
  - `1`: O instalador não verifica se a atualização do sistema operacional KB5007186 está instalada.

  Por padrão, a chave não está definida, o que corresponde a 0.

- Configuração da funcionalidade de Proteção dos serviços do sistema operacional.

  Se essa função estiver ativada, aplicativos de terceiros não poderão atuar sobre os processos do sistema operacional. Os valores possíveis para a opção `PROTECTOSSERVICES=<valor>` na linha de comando são:

  - `1` significa que a proteção dos serviços do sistema operacional está ativada (valor padrão).
  - `0` significa que a proteção dos serviços do sistema operacional está desativada.

- Configuração de portas usadas para conexão remota do Console do Aplicativo com o computador no qual o aplicativo está instalado:

  Para configurar a porta para conexão com as credenciais do Windows, é possível usar o parâmetro `UIPORT=<número da porta>`. Intervalo de números de porta possíveis: 1 a 65535. Caso o número esteja fora do intervalo especificado, o número da porta padrão será usado. O valor padrão é 13032.

  Caso necessário, é possível fechar a porta para conexão com as credenciais de usuários criados manualmente por meio do parâmetro `ENABLEUIKLPORT=<valor>`:

  - `1` abre a porta (valor padrão).
  - `0` fecha a porta.

  O valor padrão para esta porta é 13031. É possível alterar o número da porta ao especificar o parâmetro `UIKLPORT=<valor>`. O intervalo de números de porta possíveis é 1–65535.

- Configuração para ativar as conexões de rede para o gerenciamento remoto do Kaspersky Embedded Systems Security com o uso do Console de Aplicativos instalado em um computador diferente.

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

  - `1`. Caso esse valor seja especificado, as portas TCP configuradas para a conexão remota do Console do Aplicativo a um computador com o aplicativo instalado (os parâmetros `UIPORT=<valor>` e `UIKLPORT=<valor>`) serão abertas no Firewall do Windows e as conexões de rede serão permitidas para o arquivo executável do processo de gerenciamento remoto do Kaspersky Embedded Systems Security, avp.exe.

    Leia também Mais configurações para instalação do aplicativo em outro dispositivo.

  - `0`. Se esse valor for especificado, nada acontecerá.

Configurações de recuperação e opções de linha de comando do Windows Installer

- Restauração de objetos da quarentena.

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

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

- Restauração do conteúdo do backup.

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

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

- Insira a senha atual para confirmar a restauração (caso a proteção de senha esteja 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 da opção `RESTOREPATH=< caminho completo para a pasta >` na linha de comando é %ALLUSERSPROFILE%\Program Data\Kaspersky Lab\KESS.4.0.0\QB\Restored

Exemplos de comandos para instalar o Kaspersky Embedded Systems Security

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

Execute o arquivo ess_win.msi do kit de distribuição no dispositivo protegido.

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 com o uso do arquivo setup_ess.exe

Para instalar o Kaspersky Embedded Systems Security com as configurações de instalação recomendadas e sem o envolvimento do usuário:

```
\exec\setup_ess.exe EULA=1 PRIVACYPOLICY=1
```

Para instalar componentes, como o Controle de Dispositivos:

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

Ao instalar o Kaspersky Embedded Systems Security em computadores com dispositivos de rede e dispositivos SCSI que causam uma falha no sistema após a instalação, é possível usar as seguintes opções adicionais 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.

Para instalar e ativar o Kaspersky Embedded Systems Security com o uso do arquivo de chave:

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 /p LICENSEKEYPATH=C:\0000000A.key
```

Para alterar a porta usada para conexão remota do Console do Aplicativo com um computador no qual o aplicativo está instalado com as credenciais do usuário do Windows:

```
setup_ess.exe /pUIPORT=<número da porta>
```

Intervalo de números de porta possíveis: 1 a 65535. O valor padrão é 13032.

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

Para instalar o Kaspersky Embedded Systems Security com as configurações de instalação recomendadas e sem o envolvimento do usuário:

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

Para instalar o Kaspersky Embedded Systems Security com as configurações de instalação recomendadas e exibir a interface de instalação:

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

Para instalar o Kaspersky Embedded Systems Security 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:

```
msiexec /i ess_win.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 usando o arquivo de chave C:\0000000A.key:

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

Para instalar o Kaspersky Embedded Systems Security com uma verificação preliminar dos processos ativos e setores de inicialização dos discos locais:

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

Para instalar o Kaspersky Embedded Systems Security na pasta de instalação C:\KESS:

```
msiexec /i ess_win.msi INSTALLDIR=C:\KESS/qn EULA=1 PRIVACYPOLICY=1
```

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

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

Para instalar o Console do Kaspersky Embedded Systems Security:

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

Para instalar e ativar o Kaspersky Embedded Systems Security usando o arquivo de chave C:\0000000A.key e configurar o Kaspersky Embedded Systems Security de acordo com as configurações descritas no arquivo de configuração C:\settings.xml:

```
msiexec /i ess_win.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 estiver protegido por senha:

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

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

O Kaspersky Embedded Systems Security iniciará as tarefas de proteção e verificação imediatamente após a instalação se o aplicativo tiver sido ativado. Caso a caixa de seleção **Ativar a Proteção de Arquivos em Tempo Real após a instalação do aplicativo (recomendado)** tenha sido selecionada durante a instalação do Kaspersky Embedded Systems Security, o aplicativo verificará os objetos do sistema de arquivos do dispositivo quando eles forem acessados. Caso o componente de monitoramento de scripts tenha sido instalado como parte da instalação personalizada, o Kaspersky Embedded Systems Security verificará o código fonte de todos os scripts quando eles forem iniciados. O Kaspersky Embedded Systems Security 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:

- Inicie a tarefa de atualização do banco de dados do Kaspersky Embedded Systems Security. Após a instalação, o Kaspersky Embedded Systems Security 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. 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 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.

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.

Adicionar/remover componentes. Exemplos de comandos

Para instalar o componente Verificação por demanda, execute o seguinte comando:

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

ou

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

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

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

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

Para instalar novos componentes, execute o seguinte comando:

```
msiexec /i ess_win.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 instala e remove os componentes correspondentes.

Desinstalação do Kaspersky Embedded Systems Security. Exemplos de comandos

Para desinstalar o Kaspersky Embedded Systems Security do dispositivo protegido no modo silencioso, execute o seguinte comando:

```
msiexec /x ess_win.msi KLLOGIN=<user name> KLPASSWD=<password> /qn
```

ou

```
msiexec /x {70579418-34B7-49A8-A1EB-CF309F4D032B} KLLOGIN=<user name> KLPASSWD=<password>
/qn
```

ou

```
setup_ess.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

em que `<user name>` é o nome e o login de um usuário com direitos suficientes para desinstalar.

Se uma senha vazia do Windows estiver definida para a conta de usuário que realizará a remoção, desative a funcionalidade **Solicitar senha para confirmar ações críticas** antes de iniciar a remoção.

Para desinstalar o Console do Kaspersky Embedded Systems Security no modo silencioso, execute o seguinte comando:

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

ou

```
msiexec /x {D66EC1A9-A456-46FF-8B49-308A23FEBF88} /qn
```

Códigos de retorno

O instalador do aplicativo pode retornar os códigos de retorno descritos neste artigo.

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

Códigos de retorno

Código	Descrição
27100	Foram detectadas unidades com o Agente de Autenticação instalado no modo de teste no computador.
27101	Foram detectadas unidades com o Agente de Autenticação instalado no modo de teste no computador.

Código	Descrição
27102	Não foi possível encontrar discos criptografados.
27200	Não foi possível descarregar o aplicativo da RAM.
27201	Erro ao iniciar o processo AVP.exe. O computador pode estar infectado.
27204	Não foi possível armazenar o pacote em cache distribuído.
27205	Não foi possível transferir as informações de licença.
27206	Não foi possível remover as informações de licença.
27207	Não foi possível remover o software incompatível.
27208	Não foi possível verificar o software incompatível.
27209	Não foi possível extrair os arquivos do gabinete.
27210	Não foi possível configurar a Autodefesa.
27211	Não foi possível ativar a Autodefesa.
27212	Não foi possível obter as informações sobre a versão do sistema operacional.
27213	Não foi possível obter o diretório de inicialização.
27214	Não foi possível verificar o diretório de instalação.
27215	Não foi possível configurar o serviço.
27216	Não foi possível configurar a atualização do klcp.
27217	Não foi possível atualizar o klcp.
27218	Não foi possível configurar os parâmetros do driver kl1.
27219	Não foi possível configurar os parâmetros do driver klelam.
27220	Não foi possível configurar os parâmetros do driver klwfp.
27221	Não foi possível configurar o modo de compatibilidade do driver.
27222	Não foi possível remover a chave de registro.
27223	Não foi possível reiniciar o sistema operacional.
27224	Não foi possível instalar o driver.
27225	Não foi possível transferir as configurações do driver.
27226	Não foi possível interromper o driver.
27227	Não foi possível interromper a inicialização do driver.
27228	Não foi possível verificar a assinatura do arquivo.
27230	Não foi possível preparar as configurações do driver kldl.
27231	Não foi possível configurar o driver kldl.
27300	Erro na instalação do driver.
27301	Não foi possível remover o driver.
27302	Não foi possível instalar os componentes de rede.
27303	As informações de registro do driver estão inconsistentes ou incompletas. Reinicie o sistema operacional e tente novamente.
27305	Erro ao desativar o driver.
27310	Não foi possível instalar o arquivo de catálogo assinado digitalmente.
27311	Não foi possível desinstalar o arquivo de catálogo assinado digitalmente.
27312	Não foi possível instalar os certificados.
27313	Não foi possível remover os certificados.
27320	Não foi possível configurar o serviço.
27321	Não foi possível retirar a proteção do serviço.

Código	Descrição
27350	O patch <nome do patch> não visa localizar o aplicativo <nome do aplicativo>.
27352	Não foi possível remover totalmente o patch de criptografia completa do disco.
27353	O patch <nome do patch 1> só pode ser instalado em conjunto com o patch <nome do patch 2>.
27354	O computador deve ser reiniciado para aplicar os patches antes de modificar/restaurar o aplicativo.
27355	Não foi possível bloquear o gerenciamento da criptografia completa do disco. Não foi possível bloquear o gerenciamento da criptografia completa do disco. Você deve finalizar a criptografia antes de instalar uma atualização da criptografia completa do disco.
27356	Não foi possível instalar o patch.
27357	O pacote de instalação contém patches recuperados. A instalação será interrompida.
27360	Não foi possível registrar o patch.
27361	Não foi possível definir os parâmetros de instalação do patch.
27363	O patch contém bibliotecas de criptografia que não são compatíveis com as bibliotecas de criptografia instaladas.
27370	Erro ao inicializar a descompactação do .NET 8.0.
27371	Erro ao descompactar o .NET 8.0.
27372	As informações de registro da versão anterior do aplicativo foram excluídas. Reinicie a instalação.
27373	Não foi possível excluir as informações de registro sobre a versão anterior do aplicativo.
27374	O aplicativo está sendo atualizado. Tente novamente mais tarde.
27375	A senha de desinstalação ou o nome de usuário não foi especificado ou está incorreto.
27376	Não foi possível desinstalar o Kaspersky Endpoint Agent. Desinstale-o manualmente ou desative a proteção por senha nas configurações. Em seguida, reinicie a instalação do aplicativo.
27377	Não foi possível desinstalar o Kaspersky Security for Windows Server. Desinstale-o manualmente ou desative a proteção por senha nas configurações. Em seguida, reinicie a instalação do aplicativo.
27378	Espaço em disco insuficiente.
27379	Não foi possível instalar o aplicativo, porque foram selecionados componentes não compatíveis. Altere o conjunto de componentes e reinicie a instalação.
27380	Um arquivo de configuração inválido foi selecionado.
27381	Uma chave de licença inválida foi selecionada.
27382	Não foi possível criar o grupo de administração do aplicativo.
27383	Você selecionou uma pasta inválida. O nome da pasta de destino não pode ter mais de 160 caracteres.
27384	Você selecionou uma pasta ou unidade inválida. O aplicativo deve ser instalado em um disco rígido local.
27385	Você selecionou uma pasta inválida. O aplicativo não pode ser instalado na pasta raiz.
27386	Você selecionou uma pasta inválida. O aplicativo não pode ser instalado na pasta, ou subpastas, Windows.
27387	Você selecionou uma pasta inválida. O aplicativo não pode ser instalado em uma pasta que possua uma subpasta temporária.
27388	Você selecionou uma pasta inválida. O aplicativo não pode ser instalado diretamente na pasta Arquivos de Programas.
27389	Você selecionou uma pasta inválida. O aplicativo não pode ser instalado em um disco virtual.
27390	Você selecionou uma pasta ou unidade inválida. O aplicativo não pode ser instalado na mesma pasta em que sua versão anterior esteja instalada.
27391	A pasta ou unidade selecionada já possui arquivos. O aplicativo não pode ser instalado em uma pasta que contenha outros dados, porque eles podem ficar indisponíveis depois de ativar a Autodefesa.
27392	O aplicativo não pode ser instalado em uma pasta que contenha pontos de reanálise. Selecione outra pasta para a instalação.
27393	O aplicativo não pode ser instalado em uma pasta com o caractere de ponto e vírgula (;) no nome. Selecione outra pasta para a instalação.
27394	Você selecionou uma pasta inválida. Não foi possível definir a pasta raiz.
27395	Você selecionou uma pasta inválida. Não foi possível definir a pasta Windows ou suas subpastas.
27396	Você selecionou uma pasta inválida. Não foi possível definir diretamente a pasta Arquivos de programas.

Código	Descrição
27397	Você selecionou uma pasta inválida. Não foi possível definir uma pasta com uma subpasta temporária.
27400	Erro ao inicializar as atualizações do arquivo.
27450	Não foi possível instalar o arquivo CAB.
27451	Erro ao remover.
27452	Erro ao remover arquivos.
27453	Erro ao mover os arquivos.
27454	Não foi possível criar arquivos de registro.
27455	Não foi possível obter as informações sobre a versão do sistema operacional.
27456	Não foi possível programar os valores do registro de reversão.
27457	Não foi possível obter identificadores de segurança reconhecidos (SIDs).
27460	Erro ao criar descritores de segurança.
27461	Erro ao restaurar os descritores de segurança.
27462	Não foi possível criar regras para o Firewall do Microsoft Windows.
27463	Não foi possível excluir regras do Firewall do Microsoft Windows.

Instalação e desinstalação do aplicativo usando o Kaspersky Security Center

Esta seção contém informações sobre a instalação do Kaspersky Embedded Systems Security usando o Kaspersky Security Center, uma descrição do procedimento de instalação e desinstalação do Kaspersky Embedded Systems Security pelo Kaspersky Security Center e uma descrição das ações a serem executadas após o Kaspersky Embedded Systems Security ter sido instalado.

Informações gerais sobre a instalação por meio do Kaspersky Security Center

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

Após a conclusão da tarefa de instalação remota, o Kaspersky Embedded Systems Security 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 nos dispositivos protegidos desse grupo.

Você pode criar uma tarefa para instalar remotamente o Kaspersky Embedded Systems Security 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 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

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 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 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 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 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 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).

- 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 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 usando uma tarefa de instalação remota por meio do Kaspersky Security Center:

1. Abra o Console de Administração do Kaspersky Security Center.

2. No Console de Administração do Kaspersky Security Center, expanda o node **Avançado**.

3. Expanda o nó secundário **Instalação remota**.

4. No painel de resultados do nó secundário **Pacotes de instalação**, clique no botão **Criar um pacote de instalação**.

5. Selecione a opção **Criar um pacote de instalação para um aplicativo da Kaspersky**.

6. Insira o nome do novo pacote de instalação.

7. Especifique o arquivo ess_win.kud do kit de distribuição do Kaspersky Embedded Systems Security como o arquivo do pacote de instalação.

   Caso planeje instalar o aplicativo usando a configuração **Proteger o computador com bases de antivírus"** sobre a configuração do aplicativo que não usa análise de assinatura e bancos de dados de antivírus para proteger o computador, ou vice-versa, primeiramente, é necessário especificar o login e a senha da conta com permissões para instalar o aplicativo no arquivo ess_win.kud. Para fazer isso, abra o arquivo ess_win.kud em um editor de texto e adicione os seguintes parâmetros na linha `Params: /pKLLOGIN=<login>` e `/pKLPASSWD=<senha>.`

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

8. Caso concorde com os termos e condições do Contrato de Licença do Usuário Final e a Política de Privacidade, marque as caixas de seleção **Confirmo que li, entendi e aceito totalmente os termos e condições deste Contrato de Licença de Usuário Final** e **Estou ciente e aceito que meus dados sejam tratados e transmitidos (inclusive para países terceiros) como descrito na Política de Privacidade. Confirmo que li e entendi integralmente a Política de Privacidade**.

   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 e as configurações de instalação padrão no pacote de instalação:

    a. No Console de Administração do Kaspersky Security Center, expanda o node **Instalação remota**.

    b. No painel de resultados do nó secundário **Pacotes de instalação**, abra o menu de contexto do pacote de instalação do Kaspersky Embedded Systems Security criado e selecione **Propriedades**.

    c. Na janela **Propriedades: <nome do pacote de instalação>**, abra a seção **Configurações**.

    d. Selecione o tipo de instalação.

    e. Especifique a lista de exclusões para sistemas industriais clicando no botão **Configurar**.

    f. Na seção **Seleção do componente**, marque as caixas de seleção junto dos nomes dos componentes do Kaspersky Embedded Systems Security que deseja instalar.

    g. Na seção **Modo Proteção de Arquivos em Tempo Real**, marque a caixa de seleção **Ativar a Proteção de Arquivos em Tempo Real após a instalação do aplicativo (recomendado)** e especifique o nível de segurança.

    h. Caso necessário, altere os números de portas TCP usados pelo Console do Aplicativo para conexão remota ao computador com o aplicativo instalado.

    O número da porta padrão para conexão com credenciais do Windows é 13032 e o número da porta padrão para conexão com credenciais de usuários criados manualmente é 13031. Intervalo de números de porta possíveis: 1 a 65535.

    Para impedir a conexão com credenciais de contas de usuário criadas manualmente, desmarque a caixa de seleção **Uso das credenciais de usuários criados manualmente**.

    i. Para poder indicar uma pasta de destino que não seja a pasta padrão, especifique o nome da pasta e o caminho na seção **Configurar caminhos de instalação do aplicativo** clicando no botão **Configurações**.

    j. Especifique o arquivo de configuração, se aplicável.

    k. Salvar alterações.

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

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

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

Após instalar o Kaspersky Embedded Systems Security, recomendamos que você atualize os bancos de dados do Kaspersky Embedded Systems Security 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.

Se os dispositivos protegidos nos quais o Kaspersky Embedded Systems Security 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 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 agendado das tarefas de Verificação por demanda do sistema local 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.

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 nó secundário **Instalação remota**.

3. Crie um pacote de instalação:

   a. No painel de resultados do nó secundário **Pacotes de instalação**, clique no botão **Criar um pacote de instalação**.

   b. Na janela **Assistente de Novo pacote**, selecione **Criar** pacote de instalação para o arquivo executável especificado como o tipo do pacote.

   c. Insira o nome do novo pacote de instalação.

   d. Selecione o arquivo client\setup_esstool.exe na pasta do kit de distribuição do Kaspersky Embedded Systems Security e marque a caixa de seleção **Copiar toda a pasta no pacote de instalação**.

   e. No campo **Configurações de inicialização de arquivos executáveis (opcional)**, especifique os valores de parâmetros EULA=1 e PRIVACYPOLICY=1. Caso contrário, é impossível instalar componentes.

```
/s /p "EULA=1 PRIVACYPOLICY=1"
```

f. Caso seja necessário, no campo **Configurações de inicialização do arquivo executável (opcional)**, é possível especificar o parâmetro de linha de comando ADDLOCAL para modificar o conjunto de componentes a ser instalado, e o parâmetro 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 "INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=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).

5. 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.

6. Execute a tarefa de instalação remota.

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

Desinstalação do Kaspersky Embedded Systems Security através do Kaspersky Security Center

Os arquivos de despejo e rastreamento não são excluídos na desinstalação do Kaspersky Embedded Systems Security. 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 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 será desinstalado dos dispositivos nos quais a senha inserida corresponder ao valor definido. O Kaspersky Embedded Systems Security não será desinstalado de outros dispositivos protegidos.

Para desinstalar o Kaspersky Embedded Systems Security:

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 somente com as configurações de desinstalação padrão.

Alterar o conjunto de componentes de componentes de aplicativos usando o Kaspersky Security Center

A tarefa *Alterar componentes do aplicativo* permite alterar o conjunto de componentes do Kaspersky Embedded Systems Security depois que o aplicativo é instalado.

Como alterar o conjunto de componentes de aplicativos no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Tarefas**.

   A lista de tarefas é aberta.

2. Clique **Nova tarefa**.

O Assistente de Tarefas é iniciado. Siga as instruções do Assistente.

Etapa 1. Selecionar o tipo de tarefa

Selecionar **Kaspersky Embedded Systems Security for Windows (4.0) → Alterar componentes do aplicativo**.

Etapa 2. Configurações da tarefa para alterar os componentes do aplicativo

Selecione os componentes do aplicativo que estarão disponíveis no computador do usuário. Defina as configurações avançadas para a tarefa (consulte a tabela abaixo).

Etapa 3. Selecionar os dispositivos aos quais a tarefa será atribuída

Selecione os computadores nos quais a tarefa será executada. As seguintes opções estão disponíveis:

- Atribuir a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos em um grupo de administração criado anteriormente.
- Selecionar computadores detectados pelo Servidor de Administração na rede: *dispositivos não atribuídos*. Os dispositivos específicos podem incluir dispositivos nos grupos de administração e dispositivos não atribuídos.
- Especificar endereços de dispositivo manualmente ou importar endereços de uma lista. Você pode especificar nomes de NetBIOS, endereços IP e sub-redes IP de dispositivos aos quais você quer atribuir a tarefa.

Etapa 4. Configurar um agendamento de início de tarefa

Configure um agendamento para iniciar uma tarefa, por exemplo, manualmente ou quando o computador estiver ocioso.

Etapa 5. Definir o nome da tarefa

Digite um nome para a tarefa, por exemplo, *Adicionar o componente Controle de Aplicativos*.

Etapa 6. Concluir a criação da tarefa

Concluir a operação do assistente. Caso seja necessário, marque a caixa de seleção **Executar tarefa após a conclusão do assistente**. Você pode monitorar o andamento da tarefa nas propriedades da tarefa.

Como alterar o conjunto de componentes do aplicativo no Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Tarefas**.

   A lista de tarefas é aberta.

2. Clique **Adicionar**.

O Assistente de Tarefas é iniciado. Siga as instruções do Assistente.

Etapa 1. Definir as configurações gerais da tarefa

Defina as configurações gerais da tarefa:

1. Na lista suspensa **Aplicativo**, selecione **Kaspersky Embedded Systems Security 4.0.0**.
2. Na lista suspensa **Tipo de tarefa**, selecione **Alterar os componentes do Kaspersky Embedded Systems Security**.
3. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Adicionar o componente de Controle de Aplicativos*.
4. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

Etapa 2. Selecionar os dispositivos aos quais a tarefa será atribuída

Selecione os computadores nos quais a tarefa será executada. Por exemplo, selecione um grupo de administração separado ou crie uma seleção.

Etapa 3. Concluir a criação da tarefa

1. Marque a caixa de seleção **Abrir detalhes da tarefa quando a criação for concluída** e conclua o assistente.
2. Nas propriedades da tarefa, selecione a guia **Configurações do aplicativo**.
3. Selecione os componentes do aplicativo que estarão disponíveis no computador do usuário. Defina as configurações avançadas para a tarefa (consulte a tabela abaixo).

Como resultado, o conjunto de componentes do Kaspersky Embedded Systems Security nos computadores dos usuários será modificado no modo silencioso.

Configurações avançadas da tarefa

Parâmetro	Descrição
Zona confiável	Para a tarefa Alterar componentes do aplicativo, será possível adicionar apenas as exclusões de aplicativos confiáveis e de verificação na zona confiável.
Usar a senha para modificar o conjunto de componentes do aplicativo	Geralmente, os administradores ativam a Proteção por senha para restringir o acesso ao Kaspersky Embedded Systems Security. Ou seja, para modificar a seleção dos componentes do aplicativo, é necessário inserir as credenciais de um usuário que tenha a permissão **Remover/modificar/restaurar o aplicativo**. Por exemplo, é possível usar a conta KLAdmin.

Instalação e desinstalação via políticas de grupo do Active Directory

Esta seção descreve como instalar e desinstalar o Kaspersky Embedded Systems Security 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 pelas políticas de grupo.

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

Você pode instalar o Kaspersky Embedded Systems Security 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 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 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, use o pacote de instalação ess_win.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 ou o Console do Aplicativo:

1. Salve ess_win.msi em uma pasta compartilhada no controlador de 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 (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 será instalado nos dispositivos protegidos do grupo depois que tiverem sido reiniciados.

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

Após instalar o Kaspersky Embedded Systems Security 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.

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

Os arquivos de despejo e rastreamento não são excluídos na desinstalação do Kaspersky Embedded Systems Security. 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 (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 (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 usando as políticas de grupo do Active Directory.

Para desinstalar o Kaspersky Embedded Systems Security (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 ou o Console do Aplicativo.

2. Selecione a política criada para a instalação do Kaspersky Embedded Systems Security 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 (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 é removido dos dispositivos protegidos após eles serem reiniciados e antes de fazer login no Microsoft Windows.

Logs de instalação e desinstalação do Kaspersky Embedded Systems Security

Caso o Kaspersky Embedded Systems Security ou o Console do Aplicativo seja instalado ou desinstalado com o uso do assistente de instalação (desinstalação), o serviço do Windows Installer criará um log de instalação (desinstalação). Um arquivo de log nomeado kl-install-<uid>.log (em que <uid> é um identificador de log único de 8 caracteres) será salvo na pasta %temp% do usuário cuja conta foi usada para iniciar o arquivo setup_ess.exe ou setup_esstool.exe.

Se o Kaspersky Embedded Systems Security 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 e criar o arquivo de log no disco C:\, execute o seguinte comando:

```
msiexec /i ess_win.msi /l*v C:\<log_name>.log /qn EULA=1 PRIVACYPOLICY=1
```

Modificações de sistema após a instalação do Kaspersky Embedded Systems Security

Quando o Kaspersky Embedded Systems Security 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 são criadas no dispositivo protegido e no dispositivo no qual o Console do Aplicativo estiver instalado.
- Os serviços do Kaspersky Embedded Systems Security são registrados.
- O grupo de usuários do Kaspersky Embedded Systems Security é criado.
- Chaves do Kaspersky Embedded Systems Security 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 em um dispositivo protegido

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

- A pasta da instalação padrão do Kaspersky Embedded Systems Security que contém as arquivos executáveis do Kaspersky Embedded Systems Security. A seguinte pasta é especificada por padrão:

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0

- Arquivos da Management Information Base (MIB), que contêm uma descrição dos contadores e hooks publicados pelo Kaspersky Embedded Systems Security através do protocolo SNMP:

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0\mibs

- Arquivos de serviço do Kaspersky Embedded Systems Security:
  - %ProgramData%\Kaspersky Lab\KESS.4.0\Data
  - %ProgramData%\Kaspersky Lab\KESS.4.0\Settings
  - %ProgramData%\Kaspersky Lab\KESS.4.0\Dskm
- Arquivos com configurações para fontes de atualização:

  %ProgramData%\Kaspersky Lab\KESS.4.0\Data

- Atualizações de bancos de dados e módulos de software baixados usando a tarefa *Atualizar* (a pasta será criada na primeira vez que as atualizações forem baixadas usando a tarefa *Atualizar*).

  %ProgramData%\Kaspersky Lab\KESS.4.0\Update distribution

- Logs de tarefas e log de auditoria do sistema:

  %ProgramData%\Kaspersky Lab\KESS.4.0\Reports

- Conjunto de bancos de dados em uso no momento:

  %ProgramData%\Kaspersky Lab\KESS.4.0\Bases

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

  %ProgramData%\Kaspersky Lab\KESS.4.0\QB

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

  %ProgramData%\Kaspersky Lab\KESS.4.0\Data\temp\temporaryFolder

- Objetos na Quarentena (pasta padrão):

  %ProgramData%\Kaspersky Lab\KESS.4.0\QB

- Objetos no backup (pasta padrão):

  %ProgramData%\Kaspersky Lab\KESS.4.0\QB

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

  %ProgramData%\Kaspersky Lab\KESS.4.0\QB\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. A seguinte pasta é especificada por padrão:

%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools.4.0.0.

Grupo Kaspersky Embedded Systems Security

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 é instalado, as seguintes chaves do registro do sistema são criadas:

- Configurações do Kaspersky Embedded Systems Security:

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVP.ESS.4.0]

- Configurações de logs de evento do Kaspersky Embedded Systems Security (Kaspersky Event Log):

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Embedded Systems Security]

- Configurações do arquivo de rastreamento:

  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.0\Trace]

- Configurações para tarefas e funções do aplicativo:
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.0\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

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

Processos do Kaspersky Embedded Systems Security

Nome do arquivo	Finalidade
avp.exe	Fluxo de trabalho do Kaspersky Embedded Systems Security
avpsus.exe	Esse processo permite instalar e reverter atualizações críticas e aprovadas de módulos do aplicativo.

Verificação das funções do Kaspersky Embedded Systems Security. 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.

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 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 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 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.

Prefixos em arquivos EICAR

Prefixo	Status do arquivo após a verificação e a ação do Kaspersky Embedded Systems Security
Nenhum prefixo	**O Kaspersky Embedded Systems Security atribui o status Infectado ao objeto e o exclui.**
SUSP–	O Kaspersky Embedded Systems Security atribui o status **Provavelmente infectado** ao objeto detectado pelo analisador heurístico e o exclui, uma vez que objetos possivelmente infectados não são desinfectados.
WARN–	O Kaspersky Embedded Systems Security atribui o status **Provavelmente infectado** ao objeto (o código do objeto corresponde em parte ao código de uma ameaça conhecida) e o exclui, uma vez que objetos possivelmente infectados não são desinfectados.
CURE–	O Kaspersky Embedded Systems Security 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, é possível confirmar se o Kaspersky Embedded Systems Security 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 *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 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 nó **Verificação por demanda** na árvore do Console do Aplicativo.

3. Selecione o nó secundário **Verificação de áreas críticas**.

4. Adicione **Todas as unidades de rede** ao escopo da tarefa de Verificação por demanda.

5. Execute a tarefa 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 *Crítico*. O log da tarefa de Verificação por demanda tem uma nova linha com informações sobre uma ameaça no arquivo eicar.com.

Atualizar versões antigas do Kaspersky Embedded Systems Security para a versão 4.0

Ao atualizar uma versão antiga do Kaspersky Embedded Systems Security para a versão 4.0, siga estas recomendações:

- Planeje com antecedência e agende a atualização. Escolha um horário em que os servidores estejam operando com carga mais leve, por exemplo, durante o fim de semana.
- Após a atualização, ative os componentes do aplicativo um por um. Ou seja, comece, por exemplo, ativando apenas o componente Proteção de Arquivos em Tempo Real; depois ative outros componentes de proteção; então os componentes de controle e assim por diante. Recomendamos testar o aplicativo em cada etapa.
- Execute a atualização passo a passo. Primeiro, atualize um único computador; depois vários computadores; e, por último, atualize todos os computadores da organização.

Etapas do procedimento de atualização

Atualize o Kaspersky Embedded Systems Security para a versão 4.0 na seguinte ordem:

1. **Atualize o Kaspersky Security Center**

   Atualize todos os componentes do Kaspersky Security Center para a versão 14.2 ou posterior, inclusive o Agente de Rede nos computadores dos usuários e o Kaspersky Security Center no Web Console.

2. **Atualize o plug-in da Web do Kaspersky Embedded Systems Security**

   No Kaspersky Security Center Web Console, atualize o plug-in da Web do Kaspersky Embedded Systems Security para a versão 4.0.

3. **Migrar as tarefas e políticas do Kaspersky Embedded Systems Security**

   Depois de migrar políticas e tarefas, é necessário definir as configurações que o o assistente de migração não pode migrar e que não existiam em versões anteriores do aplicativo. Também recomendamos verificar se o assistente de migração migrou todas as configurações corretamente.

4. **Instale o Kaspersky Embedded Systems Security 4.0**

   O Kaspersky Embedded Systems Security versão 4.0 usa o protocolo HTTPS em vez do protocolo DCOM. Portanto, antes de instalar a nova versão do Kaspersky Embedded Systems Security, é necessário configurar o dispositivo em que o aplicativo será atualizado para ativar a inicialização remota do serviço KESS. Caso essa configuração não seja executada, o início do serviço remoto não estará disponível.

   É possível instalar o Kaspersky Embedded Systems Security 4.0 após remover uma versão anterior do aplicativo ou sobre ela.

   Ao instalar sobre uma versão mais antiga do aplicativo, o mesmo conjunto de componentes do aplicativo é instalado, levando em consideração os novos nomes e conteúdos de alguns componentes.

   Na instalação remota, o instalador instala os componentes selecionados nas propriedades do pacote de instalação.

5. **Se necessário, ative o Kaspersky Embedded Systems Security 4.0**

   Ao instalar o Kaspersky Embedded Systems Security 4.0 sobre uma versão mais antiga do aplicativo, a licença atual é automaticamente aplicada ao aplicativo e os novos componentes e tarefas do aplicativo ficam totalmente disponíveis. O prazo da licença permanece inalterado.

6. **Certifique-se de que o aplicativo esteja funcionando**

   Depois de atualizar o Kaspersky Embedded Systems Security, certifique-se de que o aplicativo esteja funcionando conforme o esperado. Certifique-se de que nenhum erro tenha sido relatado para o aplicativo; verifique também a hora da última conexão com o Servidor de Administração, a hora da última atualização e o status de proteção do computador.

   Tenha atenção à migração de listas de exclusão, aplicativos confiáveis, regras de Controle de dispositivos e regras de Controle de Inicialização de Aplicativos.

Atualização do Kaspersky Embedded Systems Security

A atualização para o Kaspersky Embedded Systems Security 4.0 é compatível com as versões 2.3, 3.1 ou posteriores. Para atualizar versões anteriores do aplicativo, você deve remover a versão instalada e instalar a versão 4.0.

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 para a versão 4.0, a versão do aplicativo instalada anteriormente é excluída automaticamente.

Ao atualizar uma instalação protegida por senha do Kaspersky Embedded Systems Security, passe a senha para o instalador de uma das seguintes formas:

- Ao instalar localmente pela interface do Assistente de Instalação ou no modo CLI interativo, especifique a senha quando solicitado.
- Ao instalar localmente no modo CLI não interativo, especifique a senha na chave `UNLOCK_PASSWORD`.
- Ao instalar o aplicativo por meio das políticas de grupo do Active Directory, especifique o valor da chave `UNLOCK_PASSWORD` no arquivo de configuração install_props.json.

Quando o aplicativo sendo atualizado remotamente através do Kaspersky Security Center é protegido por senha, é necessário primeiro desativar a proteção por senha usando uma política do Kaspersky Security Center.

Ao atualizar o aplicativo, a licença atual é automaticamente aplicada ao Kaspersky Embedded Systems Security versão 4.0, 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).

Atualização das Ferramentas de Administração do Kaspersky Embedded Systems Security

É possível atualizar o Plug-in de Administração para gerenciamento do aplicativo usando o Kaspersky Security Center para a versão 4.0 a partir das versões 2.3, 3.1, 3.2, 3.3, 3.4 ou posterior. Para atualizar versões anteriores do Plug-in de Administração e do Console de Aplicativos, é necessário remover a versão instalada e instalar a versão 4.0.

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

Para obter informações sobre como migrar as configurações do Plug-in de Administração, consulte este artigo.

Migrar as políticas e tarefas

É possível migrar as configurações de política e de tarefas de versões anteriores do aplicativo para a versão 4.0 das seguintes manerias:

- Usando o Assistente de Conversão de Políticas e Tarefas em Lotes (disponível somente no Console de Administração do Kaspersky Security Center).
- Usando o Assistente de Migração de Políticas e Tarefas do Kaspersky Embedded Systems Security 4.0 (disponível somente no Kaspersky Security Center Web Console).

É recomendável começar a migração de políticas e tarefas do Kaspersky Embedded Systems Security em um único computador. em seguida, fazê-lo em um grupo de computadores; e, por fim, concluir a migração em todos os computadores da organização.

Como usar o Assistente de Conversão de Políticas e Tarefas em Lotes para migrar as configurações de políticas e tarefas

1. No Console de administração do Kaspersky Security Center, selecione o Servidor de Administração e clique com o botão direito para abrir o menu de contexto.
2. Selecione **Todas as tarefas** → **Assistente de conversão de políticas e tarefas em lotes**.

Isso inicia o Assistente de Conversão de Políticas e Tarefas em Lotes. Siga as instruções do Assistente.

Etapa 1. Seleção do aplicativo para o qual deseja converter as políticas e tarefas

Selecione Kaspersky Embedded Systems Security 4.0. Vá para a próxima etapa.

Etapa 2. Conversão de políticas

Selecione as políticas da versão do aplicativo sendo atualizada que você deseja criar para o Kaspersky Embedded Systems Security 4.0. Vá para a próxima etapa.

Etapa 3. Conversão de tarefas

Selecione as tarefas da versão do aplicativo sendo atualizada que você deseja criar para o Kaspersky Embedded Systems Security 4.0.

As tarefas que não são de grupo (tarefas atribuídas a dispositivos individuais) não são exibidas na etapa atual.

Para converter tarefas que não são de grupo de sua versão do aplicativo para o Kaspersky Embedded Systems Security 4.0:

1. Clique **Avançar**.

   A janela **Migrar adicionalmente agendamentos e tarefas** é aberta.

2. Marque a caixa de seleção **Migrar tarefas que não são de grupo**.

3. Especifique as configurações de conexão para o Servidor de Administração do Kaspersky Security Center.

4. Clique **OK**.

Etapa 4. Conclusão do Assistente

Concluir a operação do assistente. Como resultado, o assistente faz o seguinte:

- São criadas novas políticas para o Kaspersky Embedded Systems Security 4.0.

  As novas políticas contêm configurações das políticas selecionadas do Kaspersky Embedded Systems Security , além de novas configurações introduzidas no Kaspersky Embedded Systems Security 4.0. Os nomes das novas políticas são iguais aos das políticas do Kaspersky Embedded Systems Security antes da conversão, com a adição de "(convertido)". Políticas novas têm o status *Política inativa*.

- São criadas novas tarefas para o Kaspersky Embedded Systems Security 4.0.

  As novas tarefas contêm configurações das tarefas selecionadas do Kaspersky Embedded Systems Security, além de novas configurações introduzidas no Kaspersky Embedded Systems Security 4.0. Os nomes das novas tarefas são iguais aos das tarefas do Kaspersky Embedded Systems Security antes da conversão, com a adição de "(conversão)".

- As políticas e tarefas selecionadas para conversão permanecem inalteradas.

[Como usar o assistente de migração para migrar configurações de políticas e tarefas]

Na janela principal do Web Console, selecione **Operações** → **Migração para KESS 4.0.0**.

Isso inicia a execução do assistente de migração de políticas e tarefas. Siga as instruções do Assistente.

Etapa 1. Migração da política

Selecione as políticas do Kaspersky Embedded Systems Security que deseja criar para o Kaspersky Embedded Systems Security 4.0. Vá para a próxima etapa.

Etapa 2. Migração da tarefa

Na lista de tarefas, selecione as tarefas do Kaspersky Embedded Systems Security que deseja criar para o Kaspersky Embedded Systems Security 4.0. Vá para a próxima etapa.

Etapa 3. Conclusão do Assistente

Concluir a operação do assistente. Como resultado, o assistente faz o seguinte:

- São criadas novas políticas para o Kaspersky Embedded Systems Security 4.0.

  As novas políticas contêm configurações das políticas migradas do Kaspersky Embedded Systems Security , além de novas configurações introduzidas no Kaspersky Embedded Systems Security 4.0. Os nomes das novas políticas são iguais aos das políticas do Kaspersky Embedded Systems Security antes da mesclagem, com a adição da frase "copiado do KESS". Políticas novas têm o status *Política inativa*.

- São criadas novas tarefas para o Kaspersky Embedded Systems Security 4.0.

  As novas tarefas contêm configurações das tarefas selecionadas do Kaspersky Embedded Systems Security , além de novas configurações introduzidas no Kaspersky Embedded Systems Security 4.0. Os nomes das novas tarefas são iguais aos das tarefas do Kaspersky Embedded Systems Security antes da migração, com a adição da frase "copiado do KESS".

Migração das configurações da versão do aplicativo que está sendo atualizada

As seguintes configurações são migradas sem alterações após a atualização do aplicativo e de seus plug-ins de gerenciamento para a versão 4.0:

- Configurações de componentes e tarefas, exceto os que são redefinidos para o padrão e os listados em "Limitações da migração de componentes e configurações"
- Logs de tarefas e de auditoria do sistema, bem como registros no log de eventos do Windows
- Configurações de notificações de tarefas
- Contas de usuário sob as quais as tarefas são iniciadas
- Permissões de acesso do usuário para gerenciamento do aplicativo
- Senha de conexão do servidor proxy
- Estado do atributo

As seguintes configurações são redefinidas ou definidas para os valores padrão da nova versão do aplicativo após a atualização do aplicativo e de seus plug-ins para a versão 4.0:

- 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
- Permissões para gerenciar o Kaspersky Security Service
- Configurações de aplicativos e tarefas configuradas pelo registro
- Configurações de aplicativos e tarefas que foram alteradas durante a instalação de correções críticas
- Configuração de evento
- Configurações de transferências de dados para o Servidor de Administração do Kaspersky Security Center; por padrão, a transferência de todos os dados permanece ativada
- Configurações rastreamento e dump
- Configurações das tarefas locais do aplicativo, localizadas na guia **Notificações**

As configurações que não existiam na versão do aplicativo sendo atualizada recebem valores padrão.

Limitações da migração de componentes e configurações

- O conteúdo da Quarentena da versão sendo atualizada é movido para o Backup da versão 4.0. Ao mesmo tempo, o tamanho máximo do Backup é aumentado para 400 MB e o limite de espaço disponível é aumentado para 100 MB.
- As seguintes configurações do Kaspersky Embedded Systems Security 3.4 não estão presentes nas versões 4.0 e posteriores, portanto, não são migradas: **Pasta de quarentena**, **Pasta de backup** e **Pasta para restaurar objetos**. Outras configurações existentes na versão antiga, mas não na nova versão, não são migradas.
- A lista de sessões de rede bloqueadas de computadores cliente não é migrada. Ao mesmo tempo, as configurações para desbloquear automaticamente o acesso aos recursos de arquivo de rede bloqueados permanecem inalteradas após a atualização do aplicativo.
- As configurações de proteção por senha não são migradas. No Kaspersky Embedded Systems Security 4.0, a proteção por senha passou por mudanças significativas. Caso seja necessário, ativar a proteção por senha e definir uma senha.
- Zona confiável:
  - O método de seleção de objetos da zona confiável foi alterado no Kaspersky Embedded Systems Security 4.0. As exclusões definidas como arquivos individuais ou caminhos de arquivos ou pastas podem ser migradas. As exclusões definidas como escopo predefinido (por exemplo, discos rígidos) ou uma URL de script não são migradas. Após a migração, é necessário adicionar essas exclusões manualmente.
  - Exclusões de verificação e aplicativos confiáveis predefinidos que ajudam a configurar o aplicativo nos servidores foram adicionados à zona confiável.

- Os componentes Controle de aplicativos e Controle de dispositivos foram consideravelmente reformulados. As configurações de componentes da versão sendo atualizada são migradas considerando a nova estrutura de configurações no Kaspersky Embedded Systems Security 4.0.

- As configurações dos componentes Monitor de integridade de arquivos e Monitor de acesso ao registro da versão do aplicativo sendo atualizada são migradas para as configurações do componente Monitor de integridade do sistema.

- O componente Gerenciamento de Firewall foi reprojetado no componente Firewall, que, além de fazer a interface com o firewall do Windows, agora também funciona como um firewall. Após concluir a migração, é necessário configurar o modo do componente do zero.

- Para usar a KSN, leia e aceite a Declaração da KSN novamente.

- As versões 4.0 e posteriores do aplicativo não têm suporte para o agendamento de componentes individuais. Se os componentes forem ativados, eles continuarão em execução enquanto o aplicativo estiver em execução.

- Ao migrar tarefas, a hora de início agendada para a tarefa é compensada pelo número de horas que corresponde ao número do fuso horário definido nas configurações do SO do computador em que a migração está sendo executada. Por exemplo, suponha que a hora de início da tarefa na versão anterior do aplicativo fosse 7h e o fuso horário configurado para o sistema operacional seja UTC +3:00. Então, após a migração da tarefa, a hora de início muda para 10h.

- A seção para configurar as ações a serem executadas em objetos possivelmente infectados foi removida das configurações do componente Proteção de Arquivos em Tempo Real e das tarefas de Verificação por demanda. Essas configurações não são migradas para a versão mais recente do aplicativo.

- O Kaspersky Security Center Web Console ou o Console de Administração não pode ser usado para fazer o envio para a Kaspersky analisar os objetos de Backup caso tenham sido transferidos após a atualização da versão 3.4 ou anterior do aplicativo para a versão 4.0 ou posterior.

- Ao migrar as tarefas de Verificação sob demanda, o nível de segurança padrão para escopos de verificação predefinidos muda de *Informar* para *Personalizado*.

Correspondência de componentes e tarefas no Kaspersky Embedded Systems Security versões 3.4 e 4.0

Ao atualizar o Kaspersky Embedded Systems Security 3.4 para a versão 4.0, o conjunto de componentes e tarefas é migrado apenas se o aplicativo estiver instalado localmente.

Correspondência de componentes no Kaspersky Embedded Systems Security versões 3.4 e 4.0

Componente do Kaspersky Embedded Systems Security 3.4	Componente do Kaspersky Embedded Systems Security 4.0
Zona confiável	Zona confiável
Proteção de Arquivos em Tempo Real	Proteção de Arquivos em Tempo Real
Uso da KSN	Uso da KSN
Prevenção de Exploit	Prevenção de Exploits
Scanner AMSI	Proteção AMSI
Controle de Inicialização de Aplicativos	Controle de Inicialização de Aplicativos

Componente do Kaspersky Embedded Systems Security 3.4	Componente do Kaspersky Embedded Systems Security 4.0
Controle de Dispositivos	Controle de dispositivos
Gerenciamento de Firewall	Firewall O Firewall do Windows atua como o firewall do Kaspersky Embedded Systems Security 3.4, enquanto o aplicativo gerencia o Firewall do Windows. No Kaspersky Embedded Systems Security 4.0, um componente separado é responsável pela funcionalidade de Firewall.
Proteção Contra Ameaças à Rede	Proteção Contra Ameaças à Rede
Monitor de Integridade de Arquivos	Monitor de integridade do sistema A funcionalidade dos componentes Monitor de Integridade de Arquivos e Monitor de acesso ao registro foi mesclada no componente Monitor de integridade do sistema.
Inspeção do Log	Inspeção de log
Monitor de acesso ao registro	Monitor de integridade do sistema A funcionalidade dos componentes Monitor de Integridade de Arquivos e Monitor de acesso ao registro foi mesclada no componente Monitor de integridade do sistema.
(nenhum)	Detecção de Comportamento
(nenhum)	Mecanismo de Remediação
Tarefa do Kaspersky Embedded Systems Security 3.4	**Tarefa do Kaspersky Embedded Systems Security 4.0**
Ativação do aplicativo	Ativação do aplicativo
Copiar atualizações	Atualização A funcionalidade da tarefa Copiar atualizações foi mesclada à tarefa Atualização.
Monitor de Comparação de Integridade de Arquivos	Monitor de integridade do sistema de linha de base
Atualização do Banco de Dados	Atualização A funcionalidade da tarefa Atualização do banco de dados foi mesclada à tarefa Atualização.
Atualização dos Módulos de Software	Atualização A funcionalidade da tarefa Atualização de Módulos de Software foi mesclada à tarefa Atualização.
Reversão da atualização dos bancos de dados do aplicativo	Reversão de atualização
Verificação sob demanda	Verificação por demanda
Controle de integridade de aplicativos	Controle de Integridade de Aplicativos
Gerador de Regras de Controle de Inicialização de Aplicativos	Gerador de Regras de Controle de Inicialização de Aplicativos
Gerador de Regras de Controle de Dispositivos	Gerador de Regras de Controle de Dispositivos
(nenhum)	Proteção da conexão do Servidor de Administração
(nenhum)	Alterar os componentes do Kaspersky Embedded Systems Security
(nenhum)	Redefinição do status de integridade do sistema

Interface do aplicativo

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

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

Console de Administração do Kaspersky Security Center

O Kaspersky Security Center permite instalar e desinstalar, iniciar e interromper o Kaspersky Embedded Systems Security, 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. Consulte as informações detalhadas sobre a interface do Kaspersky Security Center na *Ajuda do Kaspersky Security Center*.

Kaspersky Security Center Web Console

O Kaspersky Security Center Web Console (doravante também denominado Web Console) é um aplicativo da Web destinado a executar centralmente as principais tarefas de gerenciamento e manutenção do sistema de segurança da rede de uma organização. O Kaspersky Security Center 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*.

As seguintes ações estão disponíveis para o Web Console:

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

Trabalhar com o Plug-in de Administração

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

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

É possível gerenciar de forma centralizada vários dispositivos protegidos, que tenham o Kaspersky Embedded Systems Security instalado e que façam parte do mesmo grupo de administração, por meio do Plug-in de Administração do Kaspersky Embedded Systems Security. 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 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 no dispositivo protegido seja controlada por uma política ativa do Kaspersky Security Center.

Nenhuma ação adicional é necessária para iniciar o Plug-in de Administração do Kaspersky Embedded Systems Security no Kaspersky Security Center. Quando o plug-in de gerenciamento for instalado no dispositivo protegido do administrador, ele será iniciado juntamente com qualquer tipo de Console de Administração do Kaspersky Security Center.

O Kaspersky Embedded Systems Security 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 tarefa 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 caso o dispositivo protegido selecionado não seja controlado por uma política ativa do Kaspersky Security Center.

Gerenciamento das configurações do aplicativo

Esta seção contém informações sobre como definir as configurações gerais do Kaspersky Embedded Systems Security 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 na janela de propriedades do aplicativo

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

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 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**.
6. Clique **Propriedades**.

   A janela **Configurações** do **Kaspersky Embedded Systems Security** é exibida.
7. Ir para a seção **Configurações do aplicativo**.
8. Clique no botão **Configurações** na subseção da configuração que deseja definir.

Abertura das configurações gerais por meio da política

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

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 configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>** que se abre, vá para **Configurações do aplicativo**.
6. Clique no botão **Configurações** na subseção da configuração que deseja definir.

Definição das configurações gerais do aplicativo no Kaspersky Security Center

Você pode definir configurações gerais para o Kaspersky Embedded Systems Security 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 configurar configurações de escalabilidade e a interface do aplicativo:

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 configurar o aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para configurar uma tarefa ou aplicativo para um único dispositivo protegido, selecione a guia **Dispositivos** e acesse as configurações da tarefa local ou as configurações do aplicativo.
4. Na seção **Configurações do aplicativo**, clique no botão **Configurações** na subseção **Configurações da interface**.

5. Na janela **Configurações da interface**, na guia **Geral**, defina as seguintes configurações:

   - Na seção **Interação com o usuário**, defina se o Ícone da bandeja do sistema será exibido na barra de tarefas após a inicialização de cada aplicativo.

     - **Exibir interface do usuário**. No computador cliente, um ícone está disponível na bandeja do Windows. No menu de contexto do ícone, o usuário pode executar operações com o Kaspersky Embedded Systems Security. O Kaspersky Embedded Systems Security também exibe notificações acima do ícone do aplicativo. O menu de contexto do ícone na bandeja do sistema do Windows permite abrir a Interface Compacta de Diagnóstico. Clicar em um link na Interface Compacta de Diagnóstico abre o Console de aplicativos.

     - **Não exibir interface do usuário**. Em um computador cliente, nenhum sinal da operação do Kaspersky Embedded Systems Security é exibido. O ícone na área de notificação do Windows e as notificações não estão disponíveis.

   - Na seção **Status**, é possível especificar quais são os avisos que deseja visualizar no ícone da bandeja do sistema do Kaspersky Embedded Systems Security.

6. Clique em **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 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 configurar o aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.

   - Para configurar uma tarefa ou aplicativo para um único dispositivo protegido, selecione a guia **Dispositivos** e acesse as configurações da tarefa local ou as configurações do aplicativo.

4. Na seção **Configurações do aplicativo**, clique no botão **Configurações** na subseção **Segurança e confiabilidade**.

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

   - Na seção **Geral**, recomendamos deixar **Iniciar o aplicativo na inicialização do computador (recomendado)** ativado (padrão).

   - Na seção **Autodefesa**, ative ou desative a funcionalidade **Proteger os processos do aplicativo contra ameaças externas**.

   - Na seção **Ações ao mudar para energia de backup UPS**, especifique as limitações na carga do dispositivo protegido criadas pelo Kaspersky Embedded Systems Security após mudar para uma fonte de energia UPS:

     - **Não iniciar tarefas de verificação agendadas**

- Interromper as tarefas de verificação em execução

- Na seção **Status do computador quando as configurações são aplicadas**, configure a exibição do status de computadores cliente com o aplicativo instalado caso ocorram erros ao aplicar uma política ou executar uma tarefa.

- Na seção **Configurações de compatibilidade**, defina a configuração **Compatibilidade com ferramentas de administração remota**.

  Caso o uso do Kaspersky Embedded Systems Security juntamento com as Ferramentas de Administração Remota (RAT) cause problemas, será possível ativar o modo de compatibilidade. Os problemas podem estar relacionados à incompatibilidade das RATs com a funcionalidade Secure Desktop do aplicativo. O objetivo desta funcionalidade é confirmar as ações que podem diminuir potencialmente o nível de segurança do computador. Essa funcionalidade permite que um aplicativo exiba uma caixa de diálogo de confirmação isolada de outros processos. Essa funcionalidade utiliza direitos elevados para proteger a solicitação. Dessa forma, apenas o usuário poderá confirmar a ação e não o malware.

  Caso a caixa de seleção seja marcada, o modo de compatibilidade da RAT será ativado. O aplicativo exibe uma caixa de diálogo de confirmação sem essa funcionalidade. Isso pode reduzir o nível de segurança do computador. Não recomendamos ativar o modo de compatibilidade caso o Kaspersky Embedded Systems Security não esteja causando problemas com a sua RAT.

  Caso a caixa de seleção esteja desmarcada, o modo de compatibilidade RAT será desativado. Por padrão, a caixa de seleção fica desmarcada.

  Exemplo: ao usar o navegador no modo RemoteApp, é possível que o Kaspersky Embedded Systems Security não exiba uma janela de confirmação ao visitar um site com um certificado não confiável porque o RemoteApp não é compatível com a funcionalidade de Secure Desktop do aplicativo. Isso pode fazer com que o navegador pare de responder. Para que o navegador funcione corretamente no modo RemoteApp, é necessário ativar o modo de compatibilidade.

  Também é possível tentar ativar o modo de compatibilidade caso encontre problemas com a funcionalidade do Secure Desktop ao usar outro software de terceiros.

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

   - **Limitar a utilização da CPU para tarefas de verificação**. O Kaspersky Embedded Systems Security limita o uso da CPU do dispositivo protegido durante as tarefas de Verificação por Demanda ao valor especificado no campo **Limite superior**. A ativação dessa opção pode afetar negativamente o desempenho do Kaspersky Embedded Systems Security.

   - Conceder recursos a outros aplicativos. O consumo de recursos do computador pelo Kaspersky Embedded Systems Security ao verificá-lo pode aumentar a carga na CPU e nos subsistemas do disco rígido. Isso pode tornar outros aplicativos mais lentos. Para otimizar o desempenho, o Kaspersky Embedded Systems Security fornece um modo de transferência de recursos para outros aplicativos. Neste modo, o sistema operacional pode diminuir a prioridade das sequências da tarefa de verificação do Kaspersky Embedded Systems Security quando a carga da CPU for alta. Isso permite redistribuir recursos do sistema operacional para outros aplicativos. Assim, as tarefas de verificação receberão menos tempo da CPU. Como resultado, a verificação do computador com o Kaspersky Embedded Systems Security leva mais tempo. Por padrão, o aplicativo está configurado para conceder recursos a outros aplicativos.

7. Clique **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 aos servidores de atualização e ativação e durante a integração de aplicativos com os serviços da KSN.

Para definir as configurações de conexão, siga as etapas a seguir:

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
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 configurar o aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para configurar uma tarefa ou aplicativo para um único dispositivo protegido, selecione a guia **Dispositivos** e acesse as configurações da tarefa local ou as configurações do aplicativo.
4. Na seção **Configurações do aplicativo**, clique no botão **Configurações** na subseção **Configurações de conexão**.

   A janela **Configurações de conexão** é aberta.
5. Na janela **Configurações de conexão**, defina as seguintes configurações:
   - Na seção **Servidor proxy**, especifique as configurações do servidor proxy ao clicar no botão **Configurações**:
     - **Não usar servidor proxy**.
     - **Detectar configurações do servidor proxy automaticamente**
     - **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.
       - **Autenticação NTLM** - a autenticação será executada com o protocolo de autenticação de rede NTLM desenvolvido pela Microsoft. O modo é selecionado por padrão.
     - Insira o nome de usuário e a senha, se necessário.
     - Na seção **Licença**, marque ou desmarque a caixa de seleção **Usar o Kaspersky Security Center como servidor proxy ao ativar o aplicativo**.

- Na seção **Portas monitoradas**, especifique as portas de rede monitoradas:

  - **Monitorar todas as portas de rede**. Neste modo de monitoramento de porta de rede, os componentes de proteção monitoram os fluxos de dados transmitidos por meio de quaisquer portas de rede abertas do computador.

  - **Monitorar somente as portas de rede selecionadas**. No modo de monitoramento de porta de rede, os componentes de proteção monitoram as portas selecionadas do computador e a atividade de rede dos aplicativos selecionados. A lista de portas de rede normalmente usadas para a transmissão de e-mails e de tráfego de rede está configurada no de acordo com as recomendações dos especialistas da Kaspersky.

  Clique em **Configurações** e especifique as seguintes configurações**:**

  - **Monitorar todas as portas de aplicativos na lista recomendada pela Kaspersky**. Uma lista predefinida de aplicativos cujas portas de rede são monitoradas pelo Kaspersky Embedded Systems Security é usada. Por exemplo, a lista inclui o Google Chrome, Adobe Reader, Java e outros aplicativos.

  - **Monitorar todas as portas dos aplicativos especificados**. A lista de aplicativos cujas portas de rede são monitoradas pelo Kaspersky Embedded Systems Security.

6. Clique **OK**.

As configurações de conexão definidas são salvas.

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 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 na Inicialização do Sistema Operacional*, *Verificação de integridade do aplicativo*, *Monitor de integridade do sistema de linha de base*.
- Tarefas de atualização: *Atualização de bancos de dados e módulos do aplicativo*, *Atualização do aplicativo*.

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

Para permitir ou bloquear o gerenciamento de agendamento de inicialização para as tarefas locais do aplicativo em uma política:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados**, expanda o grupo pertinente e, no painel de resultados, selecione a guia **Políticas**.
2. Na guia **Políticas**, no menu de contexto da política para a qual deseja agendar as tarefas do sistema local do Kaspersky Embedded Systems Security para o grupo de dispositivos protegidos, selecione **Propriedades**.
3. Na janela de propriedades da política, selecione a seção **Configurações do aplicativo**.
4. Clique em **Configurações** na subseção **Executar as tarefas do sistema local**.
5. Marque a caixa de seleção **Permitir uso de tarefas locais**.
6. Use a caixa de seleção **Permitir o gerenciamento de agendamento** para permitir ou bloquear o gerenciamento de agendamento de inicialização para as tarefas locais do aplicativo.

Definição das configurações de segurança no Kaspersky Security Center

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

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
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 configurar o aplicativo para um grupo de dispositivos protegidos, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>**.
   - Para configurar uma tarefa ou aplicativo para um único dispositivo protegido, selecione a guia **Dispositivos** e acesse as configurações da tarefa local ou as configurações do aplicativo.
4. Ir para a seção **Suplementar**.
5. Clique no botão **Configurações** na subseção **Armazenamentos**.
6. Defina as configurações descritas na tabela a seguir.

Configurações de armazenamento

Parâmetro	Descrição
Na guia **Relatórios**, especifique as configurações de relatórios:	
Armazenar relatórios por no máximo	Se a caixa de seleção estiver marcada, o prazo máximo de armazenamento do relatório será limitado ao intervalo de tempo definido. O período máximo padrão de armazenamento dos relatórios é de 30 dias. Após este período, o Kaspersky Embedded Systems Security exclui as entradas mais antigas do arquivo de relatório automaticamente.
Limitar o tamanho do arquivo de relatório a	Se a caixa de seleção estiver marcada, o tamanho máximo do arquivo de relatório será limitado ao valor definido. Por padrão, o tamanho máximo de arquivo é 1024 MB. Para evitar ultrapassar o tamanho máximo do arquivo de relatório, o Kaspersky Embedded Systems Security exclui as entradas mais antigas do arquivo de relatório automaticamente quando for ultrapassado o tamanho máximo.
Na guia **Backup**, especifique as configurações de backup:	
Armazenar objetos por no máximo	Se a caixa de seleção estiver marcada, o prazo máximo de armazenamento do arquivo será limitado ao intervalo de tempo definido. O período máximo padrão de armazenamento de arquivos é de 30 dias. Depois da expiração do período máximo de armazenamento, o Kaspersky Embedded Systems Security excluirá os arquivos mais antigos do Backup.
Limitar o tamanho do backup a	Se a caixa de seleção estiver marcada, o tamanho máximo de armazenamento será limitado ao valor definido. Por padrão, a dimensão máxima é 400 MB. Para evitar ultrapassar o tamanho máximo de armazenamento, o Kaspersky Embedded Systems Security exclui os arquivos mais antigos do arquivo automaticamente quando o tamanho máximo é atingido.
Valor limite de espaço disponível	A caixa de seleção ativa ou desativa a função que monitora a quantidade mínima de espaço livre no Backup (o valor padrão é 100 MB). Se a quantidade de espaço livre ficar abaixo do limite especificado, o Kaspersky Embedded Systems Security registrará o evento *Limite de espaço disponível no Backup excedido* e emitirá uma notificação de acordo com as configurações para notificações sobre eventos desse tipo. Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security monitorará a quantidade de espaço livre no backup. A caixa de seleção **Valor limite de espaço disponível** estará ativa caso a caixa de seleção **Limitar o tamanho do backup a** seja selecionada.

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 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 está instalado.

Uma política impõe as configurações, as funções e as tarefas especificadas do Kaspersky Embedded Systems Security 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. Essas informações podem ser visualizadas no Console do Aplicativo, no node **Inspeção de log**.

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 usa os valores de configurações onde se especificou, nas propriedades da política, que **Editar proibidos**. Nesse caso, o Kaspersky Embedded Systems Security não utiliza os valores das configurações em vigor antes da aplicação da política. O Kaspersky Embedded Systems Security não aplica os valores de configurações da política ativa onde se especificou, nas propriedades da política, que **Editar permitidos**.

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 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 uma tarefa de Proteção do Computador em Tempo Real ou Proteção de Armazenamentos Conectados à Rede 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.

Criar uma política

Antes de criar uma política, é necessário instalar o plug-in de administração klcfginst.exe.

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 resultados do grupo de administração selecionado, marque a guia **Políticas** e clique no link **Criar uma política** para iniciar o assistente de política nova.

   A janela **Assistente para Novas Políticas** é exibida.
3. Na janela **Selecionar o aplicativo para o qual deseja criar uma política de grupo**, selecione Kaspersky Embedded Systems Security.
4. Clique em **Avançar**.
5. Insira um nome de política de grupo no campo **Nome**.

   O nome da política não pode conter os seguintes símbolos: `" * < : > ? \ |` .
6. Para aplicar uma configuração de política usada em uma versão anterior do aplicativo:

   a. Marque a caixa de seleção **Usar as configurações de política para uma versão anterior do aplicativo**.

   b. Clique no botão **Procurar**.

   c. Selecione a política que deseja aplicar.

   d. Clique em **Avançar**.

7. Na janela **Seleção do tipo de operação**, em **Configurações de Proteção de Arquivos em Tempo Real**, marque a caixa de seleção **Ativar Proteção de arquivos em tempo real** e especifique um nível de segurança.

   Caso o modo de execução da tarefa não seja selecionado, não será possível prosseguir para a próxima etapa do assistente de nova política.

8. Configurar a Proteção do Computador em Tempo Real.

9. Configurar as exclusões de verificação e aplicativos confiáveis.

10. 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.
    - Uma **política de ausência** é ativada quando um computador sai do perímetro da rede da organização.
    - 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**.

11. 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.

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 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)%. Status: 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 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, localizado em %Arquivos de Programas% e %Arquivos de Programas (x86)%. Status: 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, localizado nas pastas %Arquivos de programas% e %Arquivos de programas (x86)%. Status: 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).

Configuração de políticas

Para definir as configurações de política:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **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.

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

   - Selecione a opção **Propriedades** no menu de contexto da política.
   - Clique duas vezes na política selecionada.
4. Na guia **Geral** na seção **Status da política**, ative ou desative a política. Para fazer isso, selecione uma das opções a seguir:
   - **Política ativa**, caso deseje que a política seja aplicada a todos os dispositivos protegidos no grupo de administração selecionado.
   - **Política de ausência**, a política é ativada quando um computador sai do perímetro da rede da organização.
   - **Política inativa**, caso deseje ativar a política mais tarde em todos os dispositivos protegidos no grupo de administração selecionado.
5. Defina as configurações do 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.

6. Clique em **OK**.

As configurações definidas são aplicadas à política.

Indicador do nível de segurança

O indicador de nível de segurança é exibido na parte superior da janela de propriedades da política. O indicador pode assumir um dos seguintes valores:

- **Nível de proteção alto**. O indicador usa esse valor e altera sua cor para verde se todos os componentes pertencentes às seguintes categorias estiverem ativados e marcados com :
  - **Crítico**. Essa categoria inclui os seguintes componentes:
    - Proteção de Arquivos em Tempo Real.
    - Detecção de Comportamento.
    - Prevenção de Exploits.
    - Mecanismo de Remediação.
    - Ativar as notificações do Secure Desktop.
  - **Importante**. Essa categoria inclui o componente Uso da KSN.
- **Nível de proteção médio**. O indicador usa esse valor e altera sua cor para amarelo se um componente importante estiver desativado ou marcado com .
- **Nível de proteção baixo**. O indicador usa esse valor e altera sua cor para vermelho se um ou vários componentes críticos estiverem desativados ou marcados com .

Caso o indicador exiba o valor **Nível de proteção médio** ou **Nível de proteção baixo**, um link à direita do indicador abre a janela **Componentes recomendados de proteção**. Nessa janela, é possível ativar qualquer um dos componentes de proteção recomendados e impedir que eles sejam desativados.

Criando e configurando uma tarefa usando o Kaspersky Security Center

Esta seção contém informação sobre tarefas do Kaspersky Embedded Systems Security 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*
- *Proteção da conexão do Servidor de Administração*
- *Alterar os componentes do Kaspersky Embedded Systems Security*
- *Monitor de integridade do sistema de linha de base*
- *Atualização*
- *Reversão de atualização*
- *Verificação por demanda*
- *Verificação de integridade do aplicativo*
- *Remover a chave*
- *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 individual 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 nó **Seleções de dispositivos**.

É possível usar as políticas para desativar o agendamento 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, na seção **Tarefas**, clique no botão **Adicionar**.

   - Para criar uma tarefa de grupo:

     a. Expanda o nó **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 **Nova tarefa**.

   A janela do assistente de tarefa é exibida.

2. Na janela **Selecionar o tipo de tarefa**, sob o título **Kaspersky Embedded Systems Security**, selecione o tipo da tarefa a ser criada.

3. 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. 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.

     b. Defina as configurações de um recurso que reduz a carga no subsistema de disco:

     c. É possível especificar as ações que o Kaspersky Embedded Systems Security 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 receberá informações sobre as atualizações agendadas e disponíveis.

     d. Especifique o conjunto de atualizações que serão copiadas e um caminho para a pasta que será usada pelo Kaspersky Embedded Systems Security para armazenar as atualizações copiadas.

- 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.

- Criar a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos.

- Criar a tarefa de Gerador de Regras de Controle de Dispositivos.

4. Configure a programação da tarefa.

5. Clique em **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 **Selecionar uma conta para executar a tarefa**, especifique a conta que deseja usar para executar a tarefa.

8. Na janela **Definir o 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**, faça o seguinte:

   a. Marque a caixa de seleção **Executar tarefa após a conclusão do assistente** caso deseje que a tarefa inicie assim que for criada.

   b. Clique **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 nó **Dispositivos gerenciados** na árvore do Console 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 usando uma das seguintes maneiras:

   - clique duas vezes no nome do Kaspersky Embedded Systems Security
   - selecione Kaspersky Embedded Systems Security na lista e clique no botão **Propriedades**.
   - selecione o item **Propriedades** no menu de contexto do nome do Kaspersky Embedded Systems Security.

   A janela **Configurações** do **Kaspersky Embedded Systems Security** é exibida.

Configurando tarefas de grupo no Kaspersky Security Center

Para configurar a tarefa de grupo para múltiplos dispositivos protegidos:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **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 a tarefa**.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
5. Na seção **Notificação**, 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*.
6. Dependendo do tipo de tarefa configurada, execute uma das seguintes ações:
   - Para configurar a tarefa *Verificação por demanda*:
     - Na seção **Escopo da verificação**, configure um escopo de verificação.
     - Na seção **Configurações**, configure o nível de prioridade e integração de tarefa com outros componentes de software.
   - Para configurar a tarefa *Atualização*:
     - Vá para a seção **Configurações** e especifique **Configurações de atualização de bancos de dados e módulos do aplicativo**.
     - 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 *Ativação do aplicativo*:
     - Na seção **Configurações**, especifique o arquivo de chave ou o código de ativação 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 tarefa *Gerador de Regras de Controle de Dispositivos*, na seção **Configurações**, especifique as configurações que deseja usar para criar a lista de regras de Controle de Dispositivos.
7. Configure a programação da tarefa na seção **Agendamento**.

8. 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*.

9. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**. Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

10. Clique no botão **OK** na janela **Propriedades: <Nome da tarefa>**.

As recém-definidas configurações da tarefa de grupo são salvas.

As definições configuráveis das tarefas de grupo estão listadas abaixo.

- Gerador de Regras de Controle de Inicialização de Aplicativos

  Ao definir as configurações da tarefa *Gerador de Regras de Controle de Inicialização de Aplicativos*, é possível selecionar como deseja criar as regras de permissão na guia **Regras**:

  - **Criar regras de permissão com base nos aplicativos em execução**.
  - **Criar regras de permissão para aplicativos das pastas**.

  É possível especificar as seguintes ações a serem executadas durante a criação de regras de permissão do Controle de Inicialização de Aplicativos na guia **Configurações**:

  - **Usar certificado digital**
  - **Usar o assunto e a impressão digital do certificado digital**
  - **Se o certificado estiver ausente, usar**
  - **Usar hash SHA256**
  - **Gerar regras para usuários e/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 cria após a conclusão da tarefa.

  É possível definir configurações para a inicialização programada da tarefa.

- Gerador de Regras de Controle de Dispositivos

  - 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 cria após a conclusão da tarefa.
  - É possível definir configurações para a inicialização programada da tarefa.

- Ativação do aplicativo

  - Para ativar o aplicativo ou renovar a licença, é possível adicionar um arquivo de chave ou código de ativação.
  - É possível definir configurações para a inicialização programada da tarefa.

- Atualização de bancos de dados e módulos do aplicativo
  - Você pode especificar o Servidor de Administração do Kaspersky Security Center ou os servidores de atualização da Kaspersky como fonte de atualização do aplicativo no bloco de configurações **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.
  - É possível definir as configurações de um recurso que reduz a carga no subsistema do disco:
    - **Diminuir a carga na E/S de disco**
    - **RAM usada para otimização, MB**.
  - É possível especificar as ações que o Kaspersky Embedded Systems Security 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 receberá informações sobre as atualizações agendadas e disponíveis.
  - É possível especificar o conjunto de atualizações que serão copiadas e um caminho para a pasta que será usada pelo Kaspersky Embedded Systems Security para armazenar as atualizações copiadas.
  - É possível definir configurações para a inicialização programada da tarefa.
- Verificação por demanda
  - É possível especificar um escopo da verificação para a tarefa de Verificação por demanda e definir configurações de nível de segurança.
  - No bloco de configurações do **Analisador heurístico**, é possível ativar ou desativar o uso para a tarefa de Verificação por demanda e definir o nível de análise usando um controle deslizante.
  - No bloco **Integração com outros componentes**, é possível definir as seguintes configurações:
    - Inicie a tarefa de verificação no modo em segundo plano.
    - Considerar tarefa como verificação de áreas críticas.
    - Desativar a inicialização simultânea de várias tarefas de verificação.
  - É possível definir configurações para a inicialização programada da tarefa.
- Verificação de integridade do aplicativo
  - É possível definir configurações para a inicialização programada da tarefa.
- Monitor de integridade do sistema de linha de base
  - É possível configurar o modo de monitoramento e as regras que especificam as ações que serão executadas nos arquivos, no registro e nos dispositivos.
  - É possível definir configurações para a inicialização programada da tarefa.

Status da ativação do aplicativo.

Para configurar a tarefa 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.
   - 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. Na seção **Agendamento**, defina as configurações de fonte de atualização:
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.

Tarefa de atualização

Para configurar a tarefa Atualização:

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.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.

5. 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*.

6. Na seção **Configurações**, faça o seguinte:

   a. Selecione uma fonte de atualização usando o botão **Configurações** na seção **Configurações de atualização de bancos de dados e módulos do aplicativo**:

      - 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. Defina as configurações de um recurso que reduz a carga no subsistema de disco:

      - **Diminuir a carga na E/S de disco**. Essa caixa de seleção ativa ou desativa o processo em que o subsistema de disco é otimizado por meio do armazenamento de arquivos de atualização em uma unidade virtual em RAM. Por padrão, a caixa de seleção fica desmarcada.
      - **RAM usada para otimização, MB**.

   c. Especifique as ações que devem ser executadas pelo Kaspersky Embedded Systems Security quando as atualizações críticas dos módulos do aplicativo estiverem disponíveis ou quando houver informações sobre as atualizações planejadas.

   d. Especifique as configurações da cópia de atualização.

7. Configure o agendamento da tarefa na seção **Agendamento** (é possível configurar o agendamento para todos os tipos de tarefa, exceto Reversão de atualização).

8. 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*.

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

Para a tarefa de *Reversão de atualização*, é possível definir somente as configurações da 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*.

Controle de integridade de aplicativos

Para configurar a tarefa de grupo Verificação de integridade do aplicativo:

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e selecione o grupo de administração para o qual deseja configurar a tarefa Controle de Integridade de Aplicativos.
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 a tarefa do Controle de Integridade de Aplicativos 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.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
5. 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*.
6. Na seção **Dispositivos**, selecione os dispositivos para os quais você deseja configurar a tarefa de Controle de Integridade de Aplicativos.
7. Na seção **Agendamento**, defina as configurações de fonte de atualização:
8. Na seção **Conta**, especifique a conta cujos direitos serão usados para executar a tarefa.
9. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

   Para obter informações detalhadas sobre as definições das configurações nessas seções, consulte a *Ajuda do Kaspersky Security Center*.

10. Clique no botão **OK** na janela **Propriedades: <Nome da tarefa>**.

Gerenciando programações de tarefas

É possível programar as tarefas do Kaspersky Embedded Systems Security.

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 nó **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. Na lista suspensa **Início agendado**, selecione os parâmetros de inicialização:

   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.

   - **A cada N horas** se quiser que a tarefa seja executada periodicamente a cada poucas horas; digite o número de horas no campo **Intervalo de início (h)**.
   - **A cada N dias** se quiser que a tarefa seja executada periodicamente a cada poucos dias; digite o número de dias no campo **Intervalo de início (dias)**.
   - **A cada N minutos** se quiser que a tarefa seja executada periodicamente a cada poucos minutos; digite o número de minutos no campo**Intervalo de início (min.)**.
   - **Semanalmente** se quiser que a tarefa seja executada em um determinado dia da semana; também especifique a hora de execução desejada.
   - **Mensalmente** se quiser que a tarefa seja executada em um determinado dia do mês; também especifique a hora de execução desejada.
   - **Uma vez** se quiser que a tarefa seja executada uma vez na data e hora especificados.
   - **Manualmente** se quiser executar a tarefa manualmente.
   - **No início do aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security.
   - **Quando novas atualizações são baixadas no repositório** se quiser que a tarefa seja executada sempre que atualizações forem baixadas para o repositório.

- **No surto de vírus** se quiser que a tarefa seja executada quando um ataque de vírus for detectado.
- **Na conclusão de outra tarefa** se quiser que a tarefa seja executada durante a conclusão de outra tarefa.

a. Especifique a hora para a primeira inicialização da tarefa no campo **Hora de início**.

b. No campo **Plano para**, especifique a data de início da programação.

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 da tarefa**. No campo **Próximo início** 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 **Próximo início** 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.

7. Marque a caixa de seleção **Executar tarefas ignoradas** para ativar a inicialização de tarefas ignoradas.
8. Caso a caixa de seleção **Usar atraso aleatório automaticamente para início da tarefa** esteja marcada, a tarefa não é executada estritamente dentro do cronograma, mas de forma aleatória dentro de um determinado intervalo, ou seja, os horários de início da tarefa são espalhados.
9. Clique em **Avançado** para definir as configurações de agendamento de acordo com seus requisitos:
   - **Ligar dispositivos usando a função Wake-On-LAN antes de iniciar a tarefa**. Caso a caixa de seleção esteja marcada, o sistema operacional do computador receberá um tempo de espera especificado para concluir a inicialização antes que a tarefa seja executada. O de espera padrão é 5 minutos.
   - **Desligar os dispositivos após concluir a tarefa**. Caso a caixa de seleção esteja marcada, os dispositivos serão desligados após a conclusão da tarefa.
   - **Interromper a tarefa se ela durar mais do que**. Caso a caixa de seleção esteja marcada, a tarefa será interrompida se ela for executada por mais tempo do que o tempo especificado.
10. Clique **OK**.
11. 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. Selecione as configurações para executar uma tarefa agendada a partir da lista suspensa **Início agendado** caso queira ativar o início da tarefa agendada.
7. Selecione **Manualmente** na lista suspensa caso queira desativar o início da tarefa agendada.

   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.

8. Clique em **OK**.

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:

- 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

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 para cada componente: *Em execução*, *Pausado*, *Interrompido*, *Não coberto pela licença*.

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. Selecione a guia **Dispositivos**.
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 Ativa.
2. Selecione o node **Servidor de Administração <Nome do Servidor de Administração>** na árvore do Console de Administração.
3. Selecione a guia **Dispositivos**.
4. Clique duas vezes no item **Relatório de aplicativos proibidos em modo de teste**.

   Um relatório é gerado.
5. 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. Selecione a guia **Dispositivos**.
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

Esta seção fornece informações sobre o Console do Kaspersky Embedded Systems Security e descreve como gerenciar o aplicativo usando o Console do Aplicativo instalado no dispositivo protegido ou em outro dispositivo.

Abrir o Console do Aplicativo

Para iniciar o Console do Aplicativo:

1. Abra a Interface Compacta de Diagnóstico da seguinte maneira:

   - Execute o arquivo avpui.exe na pasta de instalação do aplicativo no dispositivo protegido. Por padrão, o arquivo está localizado em C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0.

   - Clique no ícone de aplicativo na área de notificação da área de tarefas.

2. Na janela aberta Interface Compacta de Diagnóstico, clique no link **Kaspersky Embedded Systems Security Console**.

   Caso já tenha configurado uma conexão com o dispositivo protegido, o Console de Aplicativos será aberto.

   Se for a sua primeira vez abrindo o Console de Aplicativos, você será levado à janela **Selecionar o dispositivo protegido**, na qual será preciso **configurar a conexão do Console de Aplicativos com o computador protegido**.

   a. Caso o Kaspersky Embedded Systems Security e o Console de aplicativos estejam instalados no mesmo computador, selecione **Computador local (o computador no qual o Console do Aplicativo está em execução)**.

   b. Caso o Kaspersky Embedded Systems Security e o Console de aplicativos estejam instalados em computadores diferentes:

      1. Selecione **Outro dispositivo**.

      2. Clique em **Procurar** e especifique o nome do computador onde o aplicativo está instalado.

      3. Insira a porta para se conectar ao computador com o aplicativo instalado.

   c. Marque ou desmarque a caixa de seleção **Conectar como usuário** para ativar ou desativar o uso de permissões de conta de usuário ao conectar o Console de Aplicativos ao computador com o aplicativo instalado.

d. Caso ative a conexão como usuário, insira o nome de usuário e senha. O usuário especificado deve ser membro do grupo Administradores do ESS no computador onde o aplicativo está instalado.

O nome de usuário diferencia maiúsculas de minúsculas.

e. Clique **Conectar**.

Interface do Console do Kaspersky Embedded Systems Security

Esta seção descreve os elementos primários da interface do aplicativo.

Janela do Console do Kaspersky Embedded Systems Security

Após estabelecer conexão com o Kaspersky Embedded Systems Security instalado em um dispositivo protegido diferente, o nome do nó é 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 <Nome do dispositivo protegido> como <nome da conta>**. Durante a conexão o Kaspersky Embedded Systems Security instalado no mesmo dispositivo protegido com o Kaspersky Embedded Systems Security Console, o nome do nó será Kaspersky Embedded Systems Security.

Árvore do Console

A árvore do Console do Aplicativo exibe o node **Kaspersky Embedded Systems Security** e os subnós dos componentes funcionais do aplicativo.

O nó **Kaspersky Embedded Systems Security** inclui os seguintes subnós:

- **Proteção do Computador em Tempo Real** permite configurar as seguintes tarefas:
  - **Proteção de Arquivos em Tempo Real**
  - **Kaspersky Security Network**
  - **Prevenção de Exploits**
  - **Proteção Contra Ameaças à Rede**
  - **Detecção de Comportamento**
  - **Mecanismo de Remediação**
  - **Proteção AMSI**.

- **Controle do Computador**: controle de aplicativos em execução no dispositivo protegido e nos dispositivos conectados.
  - **Controle de Inicialização de Aplicativos**
  - **Controle de dispositivos**
  - **Firewall**.
- **Geração de regra automática**: 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. Não é possível gerenciar tarefas de grupo pelo Kaspersky Embedded Systems Security Console.
- **Inspeção do sistema**: definição das configurações do monitor de integridade do sistema e análise do log de eventos do Windows.
  - **Inspeção de log**
  - **Monitor de integridade do sistema**.
- **Verificação por demanda**: gerencia as tarefas de Verificação por Demanda. Existe um nó separado para cada tarefa:
  - **Verificação de áreas críticas**
  - **Controle de Integridade de Aplicativos**
  - **Verificação de unidades removíveis**
  - **Verificação completa**
  - 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 para os bancos de dados do Kaspersky Embedded Systems Security, módulos de aplicativos e oferece a possibilidade de reverter a última atualização:
  - **Atualização de bancos de dados e módulos do aplicativo**
  - **Reversão da última atualização**
  - **Atualização 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**: gerencia as configurações de backup e a lista de sessões de rede bloqueadas.
  - **Backup**
  - **Sessões de rede bloqueadas**.
- **Logs e notificações**: gerencia os logs de tarefas locais e o log de auditoria do Kaspersky Embedded Systems Security System.
  - **Auditoria do Sistema**
  - **Controle de Inicialização de Aplicativos**
  - **Controle de dispositivos**
  - **Controle de Integridade de Aplicativos**
  - **Inspeção de log**
  - **Monitor de integridade do sistema**
  - **Proteção Contra Ameaças à Rede**
  - **Verificação por demanda**
  - **Firewall**
  - **Prevenção de Exploits**
  - **Detecção de Comportamento**
  - **AMSI Scanner**
  - **Atualização**
  - **Proteção de Arquivos em Tempo Real**
  - **Backup**.
- **Licença**: adiciona ou exclui as chaves do Kaspersky Embedded Systems Security 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** seja selecionado, o painel de detalhes exibirá as informações sobre o status atual da proteção do dispositivo e informações sobre o Kaspersky Embedded Systems Security, o status da proteção de seus componentes funcionais e o status da chave.

Menu de contexto do nó Kaspersky Embedded Systems Security

É possível usar os itens do menu de contexto do nó do **Kaspersky Embedded Systems Security** para executar as seguintes operações:

- **Pausar a proteção**.
- **Configurar a Zona confiável**. Visualize e defina as configurações da Zona Confiável.
- **Verificação de unidades removíveis**. Configurar a verificação de unidades removíveis conectadas ao dispositivo protegido via porta USB.
- **Permissões de acesso do usuário para gerenciamento do aplicativo**. Visualize e configure permissões de acesso a funções do Kaspersky Embedded Systems Security.
- **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service**. Visualize e configure direitos de usuário para gerenciar Kaspersky Security Service.
- **Armazenamentos**
- **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.
- **Atualizar**. Atualizar o conteúdo da janela do Console do Kaspersky Embedded Systems Security. Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.
- **Propriedades do aplicativo**. Visualize e defina as configurações do Kaspersky Embedded Systems Security ou uma tarefa selecionada. Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.

  Para fazer isso, também é possível usar o link **Propriedades do aplicativo** no painel de detalhes do nó do Kaspersky Embedded Systems Security.

- **Ajuda**. Visualize as informações na Ajuda do Kaspersky Embedded Systems Security. 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

É possível gerenciar as tarefas do aplicativo com o uso dos itens dos menus de contexto de cada tarefa na árvore do Console do Kaspersky Embedded Systems Security.

Você pode usar os itens do menu de contexto para executar as seguintes operações:

- **Reiniciar** / **Pausar**. Reiniciar ou pausar a execução da tarefa. Para executar essas operações, você também pode usar os botões da barra de ferramentas. Esta operação está disponível para as tarefas de Proteção em Tempo Real e tarefas de Verificação por Demanda.
- **Criar tarefa**. Crie uma nota tarefa personalizada.

- **Excluir tarefa**. Excluir tarefa personalizada.
- **Exportar configurações** / **Importar configurações**. Exportar ou importar configurações da tarefa.
- **Propriedades**. Abre a janela de configurações da tarefa.
- **Ajuda**. Abre o tópico correspondente da ajuda on-line.

Ícone da Bandeja do Sistema na área de notificação

Logo após a instalação do Kaspersky Embedded Systems Security, o ícone do aplicativo é exibido na área de notificação da barra de tarefas do Microsoft Windows.

Se o ícone do aplicativo na área de notificação da barra de tarefas estiver oculto, significa que o administrador desativou a exibição da interface do aplicativo na política.

O ícone atende às seguintes finalidades:

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

Os seguintes status do ícone do aplicativo são fornecidos para exibir informações operacionais do aplicativo:

- O ícone indica que os componentes de proteção de importância crítica do aplicativo estão ativos. O Kaspersky Embedded Systems Security exibirá um aviso se o usuário precisar executar uma ação, por exemplo, reiniciar o computador após atualizar o aplicativo.
- O ícone indica que os componentes de proteção de importância crítica do aplicativo estão desabilitados ou não funcionaram. Os componentes de proteção podem funcionar mal, por exemplo, se a licença expirou ou como resultado de um erro no aplicativo. O Kaspersky Embedded Systems Security exibirá um aviso com uma descrição do problema na proteção do computador.

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 (se instalado).
Abrir Interface de diagnóstico compacta	Abre a interface de diagnóstico compacta.
Sobre	Abre a janela **Sobre** que contém informações sobre o Kaspersky Embedded Systems Security. Para usuários registrados do Kaspersky Embedded Systems Security, a janela **Sobre** inclui 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**. O ícone aparecerá na área de notificação da barra de tarefas do Microsoft Windows.

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

Definindo as configurações de log por meio do Console do Aplicativo

As configurações gerais e as configurações de diagnóstico de mau funcionamento das configurações do Kaspersky Embedded Systems Security 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, ativar a recuperação de tarefas do Kaspersky Embedded Systems Security após um encerramento anormal, manter o log, ativar a criação de arquivos de despejo dos processos do Kaspersky Embedded Systems Security após um encerramento anormal e definir outras configurações gerais.

As configurações do aplicativo não podem ser definidas no Console do Kaspersky Embedded Systems Security se a política ativa do Kaspersky Security Center bloquear alterações a essas configurações.

Para definir as configurações gerais do Kaspersky Embedded Systems Security:

1. Na árvore do Console do Aplicativo, selecione o node **Kaspersky Embedded Systems Security** e execute uma das seguintes ações:

   - Clique no link **Propriedades do aplicativo** no painel de resultados do node.
   - Selecione **Propriedades do aplicativo** no menu de contexto do node.

   A janela **Propriedades do aplicativo** é aberta.

2. Na guia **Interface**, especifique que avisos deseja visualizar no ícone da bandeja do sistema do Kaspersky Embedded Systems Security.

3. Na guia **Configurações de segurança** defina as seguintes configurações:

   - Na seção **Geral**, configure a opção **Iniciar o aplicativo na inicialização do computador (recomendado)**.
   - Em **Autodefesa**, configure a proteção dos módulos do aplicativo e serviços do sistema operacional.
   - Na seção **Ações ao mudar para energia de backup UPS**, especifique as limitações na carga do dispositivo protegido criadas pelo Kaspersky Embedded Systems Security após mudar para uma fonte de energia UPS:
     - **Não iniciar tarefas de verificação agendadas**.
     - **Interromper as tarefas de verificação em execução**.

- Na seção **Configurações de compatibilidade**, defina a configuração **Compatibilidade com ferramentas de administração remota**.

  Caso o uso do Kaspersky Embedded Systems Security juntamento com as Ferramentas de Administração Remota (RAT) cause problemas, será possível ativar o modo de compatibilidade. Os problemas podem estar relacionados à incompatibilidade das RATs com a funcionalidade Secure Desktop do aplicativo. O objetivo desta funcionalidade é confirmar as ações que podem diminuir potencialmente o nível de segurança do computador. Essa funcionalidade permite que um aplicativo exiba uma caixa de diálogo de confirmação isolada de outros processos. Essa funcionalidade utiliza direitos elevados para proteger a solicitação. Dessa forma, apenas o usuário poderá confirmar a ação e não o malware.

  Caso a caixa de seleção seja marcada, o modo de compatibilidade da RAT será ativado. O aplicativo exibe uma caixa de diálogo de confirmação sem essa funcionalidade. Isso pode reduzir o nível de segurança do computador. Não recomendamos ativar o modo de compatibilidade caso o Kaspersky Embedded Systems Security não esteja causando problemas com a sua RAT.

  Caso a caixa de seleção esteja desmarcada, o modo de compatibilidade RAT será desativado. Por padrão, a caixa de seleção fica desmarcada.

  Exemplo: ao usar o navegador no modo RemoteApp, é possível que o Kaspersky Embedded Systems Security não exiba uma janela de confirmação ao visitar um site com um certificado não confiável porque o RemoteApp não é compatível com a funcionalidade de Secure Desktop do aplicativo. Isso pode fazer com que o navegador pare de responder. Para que o navegador funcione corretamente no modo RemoteApp, é necessário ativar o modo de compatibilidade.

  Também é possível tentar ativar o modo de compatibilidade caso encontre problemas com a funcionalidade do Secure Desktop ao usar outro software de terceiros.

- Na seção **Configurações da verificação**, defina o **limite de utilização da CPU para tarefas de verificação** e permita a concessão de recursos a outros aplicativos.

  O Kaspersky Embedded Systems Security limita o uso da CPU do dispositivo protegido durante as tarefas de verificação por demanda ao valor especificado no campo **Limite superior**.

  No entanto, o aplicativo pode usar muito mais tempo de CPU devido a outros componentes.

  A ativação dessa funcionalidade pode afetar negativamente o desempenho do Kaspersky Embedded Systems Security.

  Por padrão, essa função está desativada.

4. Na guia **Configurações de rede** defina as seguintes configurações:

   - Na seção **Servidor proxy**, especifique as configurações do servidor proxy: tipo de autenticação e detalhes necessários para a autenticação no servidor proxy.

   - Na seção **Porta para conexão remota**, se necessário, altere as portas usadas pelo Console do Aplicativo para se conectar a um computador com o aplicativo instalado.

     O número da porta padrão para conexão com credenciais do Windows é 13032 e o número da porta padrão para conexão com credenciais de usuários criados manualmente é 13031. Intervalo de números de porta possíveis: 1 a 65535.

O números de porta salvos anteriormente são usados até que o aplicativo seja reiniciado.

5. Na guia **Diagnóstico de mau funcionamento**, clique em **Configurações** e **configure o rastreamento** e **despejo de memória** do aplicativo.

   1. Selecione a guia **Configurações de despejo do aplicativo**.
   2. Marque ou desmarque a caixa de seleção **Criar arquivo de despejo** para ativar ou desativar o despejo de memória em caso de funcionamento incorreto.

      Por padrão, os arquivos de despejos de memória são armazenados na seguinte pasta: %ProgramData%\Kaspersky Lab\KESS.4.0\Traces. É possível especificar outro caminho.

   O campo **Pasta para rastreamento de arquivos** contém o caminho completo para a pasta local na qual o Kaspersky Embedded Systems Security salva os arquivos de rastreamento por padrão. É possível especificar outro caminho.

   1. Na lista suspensa **Nível de detalhes**, selecione o nível de detalhes das informações de depuração:

      - **Crítico** significa que o arquivo de rastreamento salva apenas as mensagens referentes aos erros fatais.
      - **Diagnóstico** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros e avisos.
      - **Importante** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros, avisos e informações adicionais.
      - **Normal** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros e avisos, além das informações sobre a operação normal do aplicativo (padrão).
      - **Detalhado** significa que o arquivo de rastreamento salva todas as informações referentes à operação do aplicativo.

      Um representante do Suporte Técnico determina o nível de detalhe necessário para solucionar qualquer problema que venha a ocorrer.

      O nível de detalhes padrão é configurado como **Normal**.

   2. 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 100 MB.

   3. 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**.

   4. 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.

O Kaspersky Embedded Systems Security grava as informações nos arquivos de rastreamento e no arquivo de despejo no formulário não criptografado. A pasta onde os arquivos são salvos; gerenciada pelas configurações do sistema operacional e do Kaspersky Embedded Systems Security. É possível configurar as permissões de acesso e permitir que apenas os usuários necessários acessem os logs, arquivos de rastreamento e de despejo.

6. Clique **OK**.

As configurações do Kaspersky Embedded Systems Security são salvas.

Gerenciando as tarefas do Kaspersky Embedded Systems Security

Esta seção contém informações sobre como criar, configurar, iniciar e interromper as tarefas do Kaspersky Embedded Systems Security.

Categorias de tarefa do Kaspersky Embedded Systems Security

As funções de Proteção do Computador em Tempo Real, Controle do Computador, Geração de Regra Automática, Inspeção do Sistema, Verificação por demanda, Proteção para Rede Industrial, Gerenciamento de Armazenamento e Atualização no Kaspersky Embedded Systems Security são implementadas como tarefas.

É possível gerenciar essas tarefas usando o menu de contexto da tarefa na árvore do Console do Kaspersky Embedded Systems Security e o painel de resultados. 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: *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. É possível alterar as configurações de todas as tarefas do sistema local, exceto a tarefa de *Reversão de atualização*. 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, é possível criar tarefas de verificação por demanda, tarefas de atualização e tarefas do monitor de integridade do sistema de linha de base. No Kaspersky Security Center, é possível criar tarefas de verificação por demanda, tarefas de atualização, etc. É possível renomear, configurar ou 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

É possível iniciar, pausar, reiniciar ou interromper as tarefas manualmente. Essas opções não estão disponíveis para todas as tarefas do Kaspersky Embedded Systems Security.

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** ou **Pausar**.

A operação é executada e registrada no log de auditoria do sistema.

Gerenciando programações de tarefas

É possível programar as tarefas do Kaspersky Embedded Systems Security.

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. Na árvore do Console, selecione a tarefa para a qual deseja configurar o agendamento.
2. No painel de resultados, clique em **Modo de execução** ou **Propriedades**.
3. Na seção **Modo de execução**, selecione **Por agendamento**.
4. Siga estas etapas para especificar as configurações de programação:
    a. Na lista suspensa **Frequência**, selecione um dos seguintes itens:
        - **Minutos** se quiser que a tarefa seja executada periodicamente a cada poucos minutos; digite o número de minutos no campo **Executar a cada <número> minuto(s)**.
        - **Horas** se quiser que a tarefa seja executada periodicamente a cada poucas horas; digite o número de horas no campo **Executar a cada <número> hora(s)**.

- **Dias** se quiser que a tarefa seja executada periodicamente a cada poucos dias; digite o número de dias no campo **Executar a cada <número> dia(s)**.
- **Em uma hora especificada** se quiser que a tarefa seja executada uma vez na data e hora especificadas.
- **Todo mês** se quiser que a tarefa seja executada todo mês. Especifique os dias do mês e a hora nos quais deseja que a tarefa seja executada (por padrão, a tarefa é executada no primeiro dia de cada mês).
- **Após iniciar o aplicativo**, se quiser que a tarefa seja executada cada vez que iniciar o Kaspersky Embedded Systems Security.

b. Especifique o período ou a data e hora do primeiro início da tarefa, dependendo da opção selecionada na primeira etapa.

c. Também é possível especificar o tempo pelo qual se deseja atrasar a execução da tarefa após iniciar o aplicativo.

d. Especifique o login e a senha para executar a tarefa.

5. Clique **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. Selecionar a tarefa necessária na árvore do Console do Aplicativo.
2. No painel de resultados, clique no link **Modo de execução**.
   A janela **Agendamento e modo de execução** é aberta.
3. Na janela aberta, na seção **Modo de execução**, execute uma das seguintes ações:
   - Marque a caixa de seleção **Manualmente** caso queira desativar a inicialização da tarefa agendada.
   - Marque a caixa de seleção **Por agendamento** caso queira ativar a inicialização da tarefa agendada.
4. Clique em **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:

- Gerador de Regras de Controle de Inicialização de Aplicativos
- Gerador de Regras de Controle de Dispositivos
- Inspeção do Log
- Verificação de integridade do aplicativo
- Atualização de bancos de dados e módulos do aplicativo
- 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.
- Tarefa **Gerador de Regras de Controle de Inicialização de Aplicativos**: caso as regras geradas tenham sido exportadas para um arquivo de configuração que não possa ser acessado pela conta do sistema (por exemplo, em uma pasta compartilhada no dispositivo protegido).

É possível iniciar as tarefas listadas com privilégios de conta do sistema. O Kaspersky Embedded Systems Security 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 acessará o dispositivo utilizando as permissões da conta **<nome do domínio \ nome_do_dispositivo>**.

Especificação de uma conta de usuário para iniciar uma tarefa

A opção para especificar uma conta no Console do Aplicativo não está disponível para todas as tarefas.

Para especificar uma conta para iniciar uma tarefa:

1. Na árvore do Console do Aplicativo, selecione a tarefa que deseja iniciar com os direitos de uma conta específica.
2. No painel de resultados, clique no link **Modo de execução**.

   A janela **Agendamento e modo de execução** é aberta.

3. Na janela exibida, na seção **Usuário**, execute as seguintes operações:

   a. Selecione a opção **Executar tarefa como**.

   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.

4. Clique em **OK**.

As configurações modificadas são salvas.

Configurações de importação e exportação

Esta seção explica como exportar as configurações do Kaspersky Embedded Systems Security. Você também aprenderá como exportar as configurações de certos componentes do aplicativo 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 para um arquivo de configuração XML e importar configurações para o Kaspersky Embedded Systems Security 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 a um arquivo, as configurações gerais do aplicativo e as configurações dos seguintes componentes e funções do Kaspersky Embedded Systems Security são salvas:

- Proteção de Arquivos em Tempo Real
- Prevenção de Exploit
- Proteção Contra Ameaças à Rede
- Detecção de Comportamento.
- Mecanismo de Remediação
- Scanner AMSI
- Controle de Inicialização de Aplicativos
- Controle de Dispositivos
- Firewall
- Gerador de Regras de Controle de Inicialização de Aplicativos

- Gerador de Regras de Controle de Dispositivos
- Inspeção do Log
- Monitor de integridade do sistema
- Verificação de áreas críticas
- Verificação de integridade do aplicativo
- Verificação de unidades removíveis
- Verificação completa
- Atualizar bancos de dados e módulos do software aplicativo
- Reversão da última atualização
- Atualização

Além disso, você pode salvar as configurações gerais do Kaspersky Embedded Systems Security 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 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 instalado nesse dispositivo protegido caso não tenha sido reinstalado ou atualizado.

Não é possível importar senhas salvas anteriormente usando o Kaspersky Embedded Systems Security 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 (por exemplo, um arquivo criado no Kaspersky Embedded Systems Security instalado com um conjunto incompleto de componentes). Depois que as configurações são importadas, somente estas configurações do Kaspersky Embedded Systems Security 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. Para exportar todas as configurações do Kaspersky Embedded Systems Security, no menu de contexto do nó do **Kaspersky Embedded Systems Security**, selecione o comando **Exportar configurações**.

Para exportar as configurações de um componente individual, clique no painel de resultados **Exportar configurações**.

> Não é possível exportar as configurações da Kaspersky Security Network. A Kaspersky Security Network deve ser configurada manualmente.

2. Na janela exibida, especifique o nome do arquivo XML para o qual você quer exportar a lista de configurações e selecione a pasta na qual você quer salvar este arquivo.

   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. Salvar o arquivo.

4. Clique no botão **OK** na subseção **A exportação das configurações foi concluída com sucesso**.

   O Kaspersky Embedded Systems Security exporta a lista de configurações para o arquivo XML.

Para exportar a lista de aplicativos confiáveis:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.

2. Selecione **Configurar a Zona confiável**.

3. A janela **Configurar a Zona confiável** é aberta.

4. Vá para a seção **Aplicativos confiáveis** e clique em **Configurações**.

   Essa ação abre uma janela que contém uma lista dos aplicativos confiáveis.

5. Selecione os aplicativos confiáveis que deseja exportar.

   Caso não selecione nenhum aplicativo confiável, o Kaspersky Embedded Systems Security exportará todos os aplicativos confiáveis.

6. Clique na seta e na lista suspensa e selecione **Exportar**.

7. Na janela aberta, insira o nome do arquivo XML para o qual deseja exportar a lista de aplicativos confiáveis e selecione a pasta na qual deseja salvar esse arquivo.

8. Salvar o arquivo.

   O Kaspersky Embedded Systems Security exporta a lista de aplicativos confiáveis para o arquivo XML.

Importando configurações

Para importar as configurações de um arquivo de configuração salvo:

1. Para importar todas as configurações do Kaspersky Embedded Systems Security, no menu de contexto do nó do **Kaspersky Embedded Systems Security**, selecione o comando **Importar configurações**.

   Para importar as configurações de um componente individual, clique em **Importar configurações** no painel de resultados.

Depois de importar as configurações gerais do Kaspersky Embedded Systems Security ou de seus componentes funcionais para o dispositivo protegido, não será possível reverter para as configurações anteriores.

As configurações da Kaspersky Security Network não podem ser importadas. A Kaspersky Security Network deve ser configurada manualmente.

2. Na janela exibida, selecione o arquivo de configuração XML do qual deseja importar as configurações e clique em **Abrir**.
3. Clique no botão **OK** na subseção **A importação das configurações foi concluída com sucesso**.
4. Na barra de ferramentas do Console do Aplicativo, clique no botão **Atualização**.

A janela do Console do Aplicativo exibe as configurações importadas.

O Kaspersky Embedded Systems Security 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 tiver sido reinstalado ou atualizado nele. Após a conclusão da importação, as senhas deverão ser inseridas manualmente.

Para importar a lista de aplicativos confiáveis:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.
2. Selecione **Configurar a Zona confiável**.
3. A janela **Configurar a Zona confiável** é aberta.
4. Vá para a seção **Aplicativos confiáveis** e clique em **Configurações**.
5. Clique na seta e na lista suspensa e selecione **Importar**.
6. Na janela exibida, selecione o arquivo XML a partir do qual deseja importar a lista de aplicativos confiáveis.
7. Abra o arquivo.

   Se o computador já tiver uma lista de aplicativos confiáveis, o Kaspersky Embedded Systems Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.
8. A lista é exibida na guia **Aplicativos confiáveis**. Clique **OK**.

Visualizando o status de proteção e as informações do Kaspersky Embedded Systems Security

Para visualizar informações sobre o status de proteção do dispositivo do Kaspersky Embedded Systems Security,

selecione o nó do **Kaspersky Embedded Systems Security** na árvore do Console do Kaspersky Embedded Systems Security.

Por padrão, as informações no painel de detalhes do Console do Kaspersky Embedded Systems Security 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** manualmente,*

selecione o comando**Atualizar** no menu de contexto do nó **Kaspersky Embedded Systems Security**.

As seguintes informações do aplicativo são exibidas no painel de detalhes do Console do Kaspersky Embedded Systems Security:

- 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 KSN** exibe o status da tarefa atual, por exemplo, *Em execução*, *Interrompido* ou *Nunca foi executada*. O indicador pode ter os seguintes valores:

- Cor verde do painel – indica que a tarefa de **Uso da KSN** está em execução e as solicitações de arquivos para status estão sendo enviadas à KSN.
- Cor amarela do painel – 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.
- Cor vermelha do painel – falha na tarefa.

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	Informações
Indicador de status de proteção do dispositivo	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: • Cor verde do painel – exibida por padrão e significa que o componente de Proteção de Arquivos em Tempo Real está instalado e a tarefa está em execução. • Cor amarela do painel: significa que o componente de Proteção de Arquivos em Tempo Real não está instalado e a tarefa de *Verificação de áreas críticas* não é realizada há muito tempo. • Cor vermelha do painel – as tarefas Proteção de Arquivos em Tempo Real não estão em execução.
Proteção de Arquivos em Tempo Real	**Status** – status atual do componente, por exemplo, *Em execução* ou *Desativado*.
Verificação de áreas críticas	**Data da última verificação** – data e hora da última Verificação de Áreas Críticas 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 realizada nos últimos 30 dias ou mais (valor padrão). Você pode alterar o limite para gerar esse evento.
Proteção Contra Ameaças à Rede	**Status** – status atual do componente, por exemplo, *Em execução* ou *Desativado*.
Prevenção de Exploits	**Status** – status atual do componente, por exemplo, *Em execução* ou *Desativado*. **Modo de operação** – um dos dois modos disponíveis para a tarefa Prevenção de Exploits: **Bloquear** ou**Informar**.
Detecção de Comportamento	**Status** – status atual do componente, por exemplo, *Em execução* ou *Desativado*. **Modo de operação** – um dos três modos disponíveis para a tarefa Detecção de Comportamento: **Excluir**, **Bloquear** ou **Informar**.

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

Seção	Informações
Indicador de status dos bancos de dados e módulos do aplicativo	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: • Cor verde do painel – 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 e módulos foi concluída com sucesso. • Cor amarela do painel – significa que os bancos de dados estão desatualizados ou que a última tarefa de atualização de banco de dados e módulos falhou. • Cor vermelha do painel – o evento *Os bancos de dados estão obsoletos* ou *Os bancos de dados estão atualizados* ocorreu.
Atualização do banco de dados	**Status do banco de dados**: uma avaliação do status de atualização do banco de dados. A opção pode ter os seguintes valores: • **Os bancos de dados estão atualizados** – os bancos de dados do aplicativo foram atualizados há no máximo 7 dias (padrão). • **Os bancos de dados estão desatualizados** – os bancos de dados de aplicativos foram atualizados entre 7 e 14 dias atrás (padrão). • **Os bancos de dados estão obsoletos** – os bancos de dados de aplicativos foram atualizados há mais de 14 dias (padrão). É possível alterar os limites para gerar os eventos *Os bancos de dados estão desatualizados* e *Os bancos de dados estão obsoletos*. **Data da versão do banco de dados** – 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** – a 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 valor no campo é exibido em vermelho se o evento *Com falha* ocorrer.

Controle

A seção **Controle** (consulte a tabela abaixo) exibe informações sobre as tarefas de Controle de Inicialização de Aplicativos, Controle de Dispositivos e Firewall.

Informações sobre o status do controle de dispositivos protegidos

Seção	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: • Cor verde do painel – exibida por padrão e significa que todos os componentes do Controle de Inicialização de Aplicativos estão instalados e que a tarefa está sendo executada no modo Ativo; a funcionalidade de Prevenção de Exploits está instalada e ativa. • O painel fica amarelo sob uma ou mais das seguintes condições: A Prevenção de Exploits não está em execução; o Controle de Inicialização de Aplicativos está em execução no modo Informar; a Prevenção de Exploits está em execução no modo Ativo e o Controle de Inicialização de Aplicativos não está em execução ou falhou. • Cor vermelha do painel – a tarefa Controle de Inicialização de Aplicativos não está em execução ou falhou, e a Prevenção de Exploits não está em execução ou está no modo **Informar**.
Controle de Inicialização de Aplicativos	**Status** – status atual do componente, por exemplo, *Em execução* ou *Desativado*. **Modo de operação** – um dos dois modos disponíveis para a tarefa Controle de Inicialização de Aplicativos: **$EntAppControl_OperatingMode_Active** ou **$EntAppControl_OperatingMode_StatisticsOnly**.
Controle de dispositivos	**Status** – status atual do componente, por exemplo, *Em execução* ou *Desativado*. **Modo de operação** – um dos dois modos disponíveis para a tarefa Controle de Dispositivos: **Por regras** ou **Informar**.
Firewall	**Status** – status atual do componente, por exemplo, *Em execução* ou *Desativado*.

Diagnóstico

A seção **Diagnóstico** (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	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: • Cor verde do painel – exibida por padrão e significa que um ou ambos os componentes de inspeção do 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; o evento *Não está em execução* ocorre. • Vermelho – uma das tarefas falhou.
Monitor de integridade do sistema	**Status** – status atual do componente, por exemplo, *Em execução* ou *Desativado*.
Inspeção de log	**Status** – status atual do componente, por exemplo, *Em execução* ou *Desativado*.

As informações sobre o licenciamento do Kaspersky Embedded Systems Security são exibidas na linha no canto inferior esquerdo no painel de detalhes do nó do **Kaspersky Embedded Systems Security**.

É possível configurar as propriedades do Kaspersky Embedded Systems Security seguindo o link Propriedades do Aplicativo.

É possível conectar a um dispositivo protegido diferente acessando o link Conectar a um computador remoto.

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 para Web Console do Kaspersky Embedded Systems Security e descreve como gerenciar o aplicativo instalado em um dispositivo protegido ou em um grupo de dispositivos protegidos.

Gerenciamento do Kaspersky Embedded Systems Security a partir do Web Console e Cloud Console

É possível gerenciar de forma centralizada vários dispositivos protegidos que tenham o Kaspersky Embedded Systems Security instalado e incluído em um grupo de administração usando o Plug-in da Web do Kaspersky Embedded Systems Security. O Kaspersky Security Center Web Console e o 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 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 no dispositivo protegido seja controlada por uma política ativa do Kaspersky Security Center.

O Kaspersky Embedded Systems Security 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 configurações de tarefa definidas localmente no Console do Aplicativo ou remotamente na janela Propriedades: <Nome do dispositivo protegido> do 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 tarefa 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 caso o dispositivo protegido selecionado não seja controlado por uma política ativa do Kaspersky Security Center.

O Kaspersky Security Center Web Console e o 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 tem as seguintes limitações em comparação ao Plug-in de Administração do Kaspersky Embedded Systems Security:

- 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 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 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 definir as configurações da interface do aplicativo:

1. Na janela principal do Web Console, selecione **Ativos (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 em **Configurar** na subseção **Configurações da interface**.
6. Defina as configurações descritas na tabela a seguir.

Configurações de interação do usuário e configurações de verificação

Parâmetro	Descrição
Interação com o usuário	**Não exibir interface do usuário**. Em um computador cliente, nenhum sinal da operação do Kaspersky Embedded Systems Security é exibido. O ícone na área de notificação do Windows e as notificações não estão disponíveis. **Exibir interface do usuário**. No computador cliente, um ícone está disponível na bandeja do Windows. No menu de contexto do ícone, o usuário pode executar operações com o Kaspersky Embedded Systems Security. O Kaspersky Embedded Systems Security também exibe notificações acima do ícone do aplicativo. O menu de contexto do ícone na bandeja do sistema do Windows permite abrir a Interface Compacta de Diagnóstico. Clicar em um link na Interface Compacta de Diagnóstico abre o Console de aplicativos.
Mostrar o status do aplicativo na área de notificações	Marque as caixas de seleção opostas às categorias de eventos sobre os quais deseja ver notificações na área de notificação do Microsoft Windows.

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 Web Console, selecione **Ativos (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 em **Configurar** na subseção **Segurança e confiabilidade**.
6. Defina as configurações descritas na tabela a seguir.

Configurações de segurança e confiabilidade

Parâmetro	Descrição
Iniciar o aplicativo na inicialização do computador (recomendado)	Quando a caixa de seleção é marcada, o Kaspersky Embedded Systems Security é iniciado após o carregamento do sistema operacional, protegendo o computador durante a sessão inteira. Quando a caixa de seleção é desmarcada, o Kaspersky Embedded Systems Security não é iniciado após o carregamento do sistema operacional, até que o usuário o inicie manualmente. A proteção do computador é desativada e os dados de usuário podem ser expostos a ameaças.
Proteger os processos do aplicativo contra ameaças externas	Quando essa caixa de seleção está marcada, o Kaspersky Embedded Systems Security impede que haja alteração ou exclusão de arquivos no disco rígido, processos na memória e entradas no registro do sistema.
Proteja os serviços do sistema operacional	Se a proteção dos serviços do sistema operacional estiver ativada, os aplicativos de terceiros não podem agir sobre os processos do sistema operacional. Se a proteção dos serviços do sistema operacional estiver desativada, os aplicativos de terceiros podem agir sobre os processos do sistema operacional.

Parâmetro	Descrição
Adiar tarefas agendadas quando estiver em modo de bateria	Se a caixa de seleção for marcada, o modo de conservação de energia será ativado. O Kaspersky Embedded Systems Security adia tarefas agendadas. Você pode iniciar tarefas de verificação e de atualização manualmente, se necessário. Quando o modo de conservação de energia é ativado e o computador estiver sendo executado no modo de energia da bateria, as seguintes tarefas não serão executadas mesmo se agendadas: • *Atualização de bancos de dados e módulos do aplicativo* • *Verificação completa* • *Verificação de áreas críticas* • *Verificação personalizada* • *Verificação de integridade do aplicativo* • *Verificação de IOC*.
Status do computador quando as configurações são aplicadas	Configurações para exibir os status de computadores clientes com o Kaspersky Embedded Systems Security instalado no Web Console quando ocorrem erros ao aplicar uma política ou executar uma tarefa. Os seguintes status estão disponíveis: *OK*, *Aviso* e *Crítico*.
Compatibilidade com ferramentas de administração remota	Caso o uso do Kaspersky Embedded Systems Security juntamento com as Ferramentas de Administração Remota (RAT) cause problemas, será possível ativar o modo de compatibilidade. Os problemas podem estar relacionados à incompatibilidade das RATs com a funcionalidade Secure Desktop do aplicativo. O objetivo desta funcionalidade é confirmar as ações que podem diminuir potencialmente o nível de segurança do computador. Essa funcionalidade permite que um aplicativo exiba uma caixa de diálogo de confirmação isolada de outros processos. Essa funcionalidade utiliza direitos elevados para proteger a solicitação. Dessa forma, apenas o usuário poderá confirmar a ação e não o malware. Caso a caixa de seleção seja marcada, o modo de compatibilidade da RAT será ativado. O aplicativo exibe uma caixa de diálogo de confirmação sem essa funcionalidade. Isso pode reduzir o nível de segurança do computador. Não recomendamos ativar o modo de compatibilidade caso o Kaspersky Embedded Systems Security não esteja causando problemas com a sua RAT. Caso a caixa de seleção esteja desmarcada, o modo de compatibilidade RAT será desativado. Por padrão, a caixa de seleção fica desmarcada. Exemplo: ao usar o navegador no modo RemoteApp, é possível que o Kaspersky Embedded Systems Security não exiba uma janela de confirmação ao visitar um site com um certificado não confiável porque o RemoteApp não é compatível com a funcionalidade de Secure Desktop do aplicativo. Isso pode fazer com que o navegador pare de responder. Para que o navegador funcione corretamente no modo RemoteApp, é necessário ativar o modo de compatibilidade. Também é possível tentar ativar o modo de compatibilidade caso encontre problemas com a funcionalidade do Secure Desktop ao usar outro software de terceiros.
Limitar a utilização da CPU para tarefas de verificação	O Kaspersky Embedded Systems Security limita o uso da CPU do dispositivo protegido durante as tarefas de verificação por demanda ao valor especificado no campo **Limite superior**. No entanto, o aplicativo pode usar muito mais tempo de CPU devido a outros componentes. A ativação dessa funcionalidade pode afetar negativamente o desempenho do Kaspersky Embedded Systems Security. Por padrão, essa função está desativada.
Conceder recursos a outros aplicativos	O consumo de recursos do computador pelo Kaspersky Embedded Systems Security ao verificá-lo pode aumentar a carga na CPU e nos subsistemas do disco rígido. Isso pode tornar outros aplicativos mais lentos. Para otimizar o desempenho, o Kaspersky Embedded Systems Security fornece um modo de transferência de recursos para outros aplicativos. Neste modo, o sistema operacional pode diminuir a prioridade das sequências da tarefa de verificação do Kaspersky Embedded Systems Security quando a carga da CPU for alta. Isso permite redistribuir recursos do sistema operacional para outros aplicativos. Assim, as tarefas de verificação receberão menos tempo da CPU. Como resultado, a verificação do computador com o Kaspersky Embedded Systems Security leva mais tempo. Por padrão, o aplicativo está configurado para conceder recursos a outros aplicativos.

Definição das configurações de conexão no plug-in da Web

As configurações de conexão definidas são usadas para conectar o Kaspersky Embedded Systems Security 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 Web Console, selecione **Ativos (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 em **Configurar** na subseção **Configurações de conexão**.
6. Defina as configurações descritas na tabela a seguir.

Configurações de conexão

Parâmetro	Descrição
Limitar o tráfego em uma conexão medida	Se essa caixa de seleção estiver marcada, o aplicativo limitará o tráfego de rede quando a conexão com a Internet for limitada. O Kaspersky Embedded Systems Security identifica uma conexão móvel com a Internet de alta velocidade como limitada e identifica uma conexão Wi-Fi como ilimitada. O Controle de custos de rede funciona em computadores que executam o Windows 8 ou posterior.
Não usar servidor proxy	Se esta opção estiver selecionada, o Kaspersky Embedded Systems Security conecta-se a serviços da KSN diretamente, sem usar nenhum servidor proxy.
Detectar configurações do servidor proxy automaticamente	Caso essa opção esteja selecionada, o Kaspersky Embedded Systems Security definirá automaticamente as configurações do servidor proxy.
Usar o servidor proxy especificado	Se esta opção estiver selecionada, o Kaspersky Embedded Systems Security se conectará a KSN usando configurações de servidor proxy especificadas manualmente.
Ignorar 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 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 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.
Autenticação NTLM	A autenticação será executada com o protocolo de autenticação de rede NTLM desenvolvido pela Microsoft. O modo é selecionado por padrão.
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.
Nome de usuário e senha	A autenticação é realizada usando o nome de usuário e a senha.
Monitorar todas as portas de rede	Neste modo de monitoramento de porta de rede, os componentes de proteção monitoram os fluxos de dados transmitidos por meio de quaisquer portas de rede abertas do computador.

Parâmetro	Descrição
Monitorar somente as portas de rede selecionadas	No modo de monitoramento de porta de rede, os componentes de proteção monitoram as portas selecionadas do computador e a atividade de rede dos aplicativos selecionados. A lista de portas de rede normalmente usadas para a transmissão de e-mails e de tráfego de rede está configurada no de acordo com as recomendações dos especialistas da Kaspersky.
Usar o Kaspersky Security Center como servidor proxy ao ativar o aplicativo	indique se o Kaspersky Security Center será usado como um servidor proxy para a ativação do aplicativo.

Configuração da inicialização agendada de tarefas locais no plug-in da Web

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 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 na Inicialização do Sistema Operacional*, *Verificação de integridade do aplicativo*, *Monitor de integridade do sistema de linha de base*.
- Tarefas de atualização: atualização de bancos de dados e módulos do aplicativo, Atualização do aplicativo.

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 em uma política:

1. Na janela principal do Web Console, selecione **Ativos (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 em **Configurar** na subseção **Executar as tarefas do sistema local**.

6. Defina as configurações descritas na tabela a seguir.

Configurações para a inicialização de tarefas locais

Parâmetro	Descrição
Permitir uso de tarefas locais	Se a caixa de seleção for marcada, as tarefas locais serão exibidas na interface local do Kaspersky Embedded Systems Security. Quando não há restrições de política adicionais, o usuário pode configurar e executar tarefas. No entanto, a configuração do agendamento de execução de tarefas permanece indisponível ao usuário. O usuário pode executar as tarefas apenas manualmente. Se a caixa de seleção for desmarcada, o uso de tarefas locais será interrompido. Neste modo, as tarefas locais não são executadas de acordo com o agendamento. As tarefas não podem ser iniciadas nem configuradas na interface local do Kaspersky Embedded Systems Security, ou ao trabalhar com a linha de comando.
Permitir o gerenciamento de agendamento	A caixa de seleção **Permitir uso de tarefas locais** estará ativa caso a caixa de seleção seja marcada. Caso a caixa de seleção seja marcada, o gerenciamento de agendamento ficará disponível nas propriedades da tarefa local no Console de Aplicativos. Por padrão, a caixa de seleção fica desmarcada.
Permitir que as tarefas do grupo sejam exibidas	Se a caixa de seleção for marcada, as tarefas de grupo serão exibidas na interface local do Kaspersky Embedded Systems Security. O usuário pode visualizar a lista de todas as tarefas no Console do Aplicativo. Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security exibe uma lista de tarefas vazia.
Permitir gerenciamento de tarefas do grupo	Se a caixa de seleção estiver marcada, os usuários podem iniciar e interromper as tarefas de grupo especificadas no Kaspersky Security Center. Os usuários podem iniciar e parar tarefas no Console do Aplicativo ou na interface simplificada do aplicativo. Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security inicia tarefas agendadas automaticamente ou o administrador inicia tarefas manualmente no Kaspersky Security Center.

Definição das configurações de conexão no plug-in da Web

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

1. Na janela principal do Web Console, selecione **Ativos (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 em **Configurar** na subseção **Armazenamentos**.

6. Defina as configurações descritas na tabela a seguir.

Configurações de armazenamento

Parâmetro	Descrição
Na guia **Relatórios**, especifique as configurações de relatórios:	
Armazenar relatórios por no máximo	Se a caixa de seleção estiver marcada, o prazo máximo de armazenamento do relatório será limitado ao intervalo de tempo definido. O período máximo padrão de armazenamento dos relatórios é de 30 dias. Após este período, o Kaspersky Embedded Systems Security exclui as entradas mais antigas do arquivo de relatório automaticamente.
Limitar o tamanho do arquivo de relatório a	Se a caixa de seleção estiver marcada, o tamanho máximo do arquivo de relatório será limitado ao valor definido. Por padrão, o tamanho máximo de arquivo é 1024 MB. Para evitar ultrapassar o tamanho máximo do arquivo de relatório, o Kaspersky Embedded Systems Security exclui as entradas mais antigas do arquivo de relatório automaticamente quando for ultrapassado o tamanho máximo.
Na guia **Backup**, especifique as configurações de backup:	

Parâmetro	Descrição
Armazenar objetos por no máximo	Se a caixa de seleção estiver marcada, o prazo máximo de armazenamento do arquivo será limitado ao intervalo de tempo definido. O período máximo padrão de armazenamento de arquivos é de 30 dias. Depois da expiração do período máximo de armazenamento, o Kaspersky Embedded Systems Security excluirá os arquivos mais antigos do Backup.
Limitar o tamanho do backup a	Se a caixa de seleção estiver marcada, o tamanho máximo de armazenamento será limitado ao valor definido. Por padrão, a dimensão máxima é 400 MB. Para evitar ultrapassar o tamanho máximo de armazenamento, o Kaspersky Embedded Systems Security exclui os arquivos mais antigos do arquivo automaticamente quando o tamanho máximo é atingido.
Valor limite de espaço disponível	A caixa de seleção ativa ou desativa a função que monitora a quantidade mínima de espaço livre no Backup (o valor padrão é 100 MB). Se a quantidade de espaço ficar abaixo do limite especificado, o Kaspersky Embedded Systems Security registrará o evento Limite de espaço livre no Backup excedido e emitirá uma notificação de acordo com as configurações para notificações sobre eventos desse tipo. Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security monitorará a quantidade de espaço livre no backup. A caixa de seleção **Valor limite de espaço disponível** estará ativa caso a caixa de seleção **Limitar o tamanho do backup a** seja selecionada. A caixa de seleção é marcada por padrão.

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 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 está instalado.

Uma política impõe as configurações, as funções e as tarefas especificadas do Kaspersky Embedded Systems Security 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 Web Console.

As informações sobre a imposição da política são registradas no log de auditoria do sistema do Kaspersky Embedded Systems Security. Essas informações podem ser visualizadas no Console do Aplicativo, no node **Registros e notificações**.

O Kaspersky Security Center oferece uma maneira para aplicar políticas em computadores locais: Proibir a alteração das configurações.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 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 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.

Como criar uma política no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique **Adicionar**.
3. A janela **Nova política** é aberta.
4. Na seção **Selecione o aplicativo**, selecione Kaspersky Embedded Systems Security.
5. Especificar os modos do Kaspersky Embedded Systems Security em dispositivos protegidos.
6. Caso seja necessário, especifique arquivos ou pastas, além de nomes de objetos (de acordo com a enciclopédia de vírus) que gostaria de excluir da verificação por todos ou alguns componentes do aplicativo.
7. Na guia **Geral**, você pode executar as seguintes ações:
   - Alterar o nome da política.

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

   - Selecionar o status da política:
     - **Ativo**. Depois da sincronização seguinte, a política será usada como a política ativa no computador.
     - **Inativo**. Política de reserva. Se necessário, uma política inativa pode ser trocada para o status ativo.
     - **Fora do escritório**. A política é ativada quando um computador sai do perímetro da rede da organização.
   - Configurar a herança de configurações:
     - **Herdar configurações da política principal**. Se esse botão de alternância estiver ativado, os valores da configuração da política serão herdados da política de nível superior. As configurações da política não poderão ser editadas se for definido para a política principal.
     - **Forçar herança de configurações nas políticas secundárias**. Se o botão de alternância 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 para as configurações marcadas com . As configurações da política secundária não poderão ser editadas se for definido para a política principal.
8. Na guia **Configurações do aplicativo**, configure a política conforme necessário.
9. Clique **Salvar**.

A **política criada** é exibida na lista de políticas da 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.

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 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)%. Status: 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 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, localizado em %Arquivos de Programas% e %Arquivos de Programas (x86)%. Status: 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, localizado nas pastas %Arquivos de programas% e %Arquivos de programas (x86)%. Status: 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).

Criando e configurando uma tarefa usando o Kaspersky Security Center

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

Sobre a criação de tarefas no plug-in da Web

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

- Para um único dispositivo protegido: na janela **<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 nó **Seleções de dispositivos**.

É possível usar as políticas para desativar o agendamento 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 da Web 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 **Ativos (dispositivos)** → **Dispositivos gerenciados**.
     b. Clique no nome do dispositivo protegido.
     c. Na janela **<Nome do dispositivo>** que é exibida, selecione a guia **Tarefas**.
     d. Clique **Adicionar**.
   - Para criar uma tarefa de grupo:
     a. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Tarefas**.
     b. Clique **Adicionar**.

   A janela do assistente de tarefa é exibida.
2. Na lista suspensa **Aplicativo**, selecione **Kaspersky Embedded Systems Security**.
3. Na lista suspensa **Tipo de tarefa**, selecione o tipo de tarefa que deseja criar.

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. 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 **Fontes 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.

     b. Defina as configurações de um recurso que reduz a carga no subsistema de disco:

     c. É possível especificar as ações que o Kaspersky Embedded Systems Security 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 receberá informações sobre as atualizações agendadas e disponíveis.

     d. Especifique o conjunto de atualizações que serão copiadas e um caminho para a pasta que será usada pelo Kaspersky Embedded Systems Security para armazenar as atualizações copiadas.

   - Para criar a tarefa de Ativação do aplicativo:

     a. Na janela **Selecionar uma chave de licença**, especifique o arquivo de chave que deseja usar para ativar o aplicativo.

     b. Marque a caixa de seleção **Usar como uma chave reserva** se desejar criar uma tarefa para renovar a licença.

   - Criar e configurar a tarefa de Gerador de Regras de Controle de Inicialização de Aplicativos.
   - Criar e configurar a tarefa de Gerador de Regras de Controle de Dispositivos.

5. Clique **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 **Avançar**.

8. Na janela **Concluir a criação da tarefa**, marque a caixa de seleção **Abrir detalhes da tarefa quando a criação for concluída** caso deseje configurar a tarefa.

9. Clique **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 **Ativos (dispositivos)** → **Tarefas**.
2. Clique no nome da tarefa na lista de tarefas do Kaspersky Security Center.

   A janela **<Nome da tarefa>** é exibida.
3. Vá para a guia **Configurações do aplicativo**.
4. Dependendo do tipo de tarefa configurada, execute uma das seguintes ações:

   - Para configurar a tarefa *Verificação por demanda*:

     a. Na seção **Escopo da verificação**, configure um escopo de verificação.

     b. Na seção **Opções**, configure o nível de análise heurística e integração com outros componentes do aplicativo.

   - Para configurar a tarefa *Atualização*, ajuste as configurações da tarefa de acordo com suas necessidades:

     a. Na seção **Fontes de atualização**, defina as configurações de fonte de atualização:

     b. Na seção **Configurações da atualização**, gerencie as configurações de otimização do subsistema de disco, especifique as ações que deseja que sejam executadas pelo Kaspersky Embedded Systems Security caso as atualizações críticas de módulos de aplicativos estejam disponíveis ou caso haja informações sobre as atualizações planejadas; especifique as configurações de cópia de atualização.

   - Para configurar a tarefa de *Ativação do aplicativo*, aplique o arquivo de chave ou código de ativação 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.
5. Configure o agendamento da tarefa na seção **Agendamento** (é possível configurar o agendamento para todos os tipos de tarefa, exceto *Reversão de atualização*).
6. 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*.
7. Clique **Salvar**.

As recém-definidas configurações da tarefa de grupo são salvas.

Configuração da tarefa de ativação do aplicativo no plug-in da Web

Para configurar a tarefa Ativação do aplicativo:

1. Na janela principal do Web Console, selecione **Ativos (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 **Configurações do aplicativo**, especifique o arquivo de chave que deseja usar para ativar o aplicativo. Marque a caixa de seleção **Usar como uma chave reserva** 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 **Salvar**.

Configuração das tarefas de Atualização no plug-in da Web

Para configurar a tarefa Atualização:

1. Na janela principal do Web Console, selecionar **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 guia **Configurações do aplicativo**.
4. Na seção **Fontes de atualização**, defina as configurações de fonte de atualização:

   a. 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.

   b. Defina as configurações de um recurso que reduz a carga no subsistema de disco:

   - Diminuir a carga na E/S de disco
   - RAM usada para otimização, MB

   c. Especifique as ações que devem ser executadas pelo Kaspersky Embedded Systems Security quando as atualizações críticas dos módulos do aplicativo estiverem disponíveis ou quando houver informações sobre as atualizações planejadas.

   d. Especifique as configurações da cópia de atualização.

5. Configure o agendamento da tarefa na seção **Agendamento** (é possível configurar o agendamento para todos os tipos de tarefa, exceto *Reversão de atualização*).

6. Na janela **<Nome da tarefa>**, clique em **OK**.

Gerenciando programações de tarefas

É possível programar as tarefas do Kaspersky Embedded Systems Security.

Programação de tarefas

É possível agendar as tarefas locais do sistema e as tarefas personalizadas no Web Console.

Para agendar as tarefas de grupo usando o Web Console:

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Tarefas**.

2. Clique no nome da tarefa na lista de tarefas do Kaspersky Security Center.

   A janela **<Nome da tarefa>** é exibida.

3. Vá para a seção **Agendamento** e configure o agendamento conforme necessário.

   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.

   a. Na lista suspensa **Iniciar tarefa**, selecione um dos seguintes itens:

   - **A cada N horas** se quiser que a tarefa seja executada periodicamente a cada poucas horas; digite o número de horas no campo **Intervalo**.
   - **A cada N dias** se quiser que a tarefa seja executada periodicamente a cada poucos dias; digite o número de dias no campo **Intervalo**.
   - **A cada N minutos** se quiser que a tarefa seja executada periodicamente a cada poucos minutos; digite o número de minutos no campo**Intervalo**.
   - **Por dias da semana** se quiser que a tarefa seja executada em um determinado dia da semana; também especifique a hora de execução desejada.

     No Kaspersky Security Center 15.1, é possível executar tarefas em intervalos de várias semanas (o parâmetro **Período**). O Kaspersky Embedded Systems Security não é compatível com a execução de tarefas em intervalos de várias semanas. Caso tenha uma tarefa agendada para executar em um intervalo de várias semanas para o Kaspersky Embedded Systems Security, o aplicativo executará a tarefa todas as semanas no dia e hora especificados.

   - **Mensalmente** se quiser que a tarefa seja executada em um determinado dia do mês; também especifique a hora de execução desejada.

- **Uma vez** se quiser que a tarefa seja executada uma vez na data e hora especificados.
- **Manualmente** se quiser executar a tarefa manualmente.
- **No início do aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security.
- **Quando novas atualizações são baixadas no repositório** se quiser que a tarefa seja executada sempre que atualizações forem baixadas para o repositório.
- **No surto de vírus** se quiser que a tarefa seja executada quando um ataque de vírus for detectado.
- **Na conclusão de outra tarefa** se quiser que a tarefa seja executada durante a conclusão de outra tarefa.

b. Nos campos **Hora de início** e **Data**, especifique a hora de início da primeira tarefa.

4. No bloco **Configurações adicionais**:
   - Marque a caixa de seleção **Executar tarefas ignoradas** para ativar a inicialização de tarefas ignoradas.
   - Caso a caixa de seleção **Usar atraso aleatório automaticamente para início da tarefa** esteja marcada, a tarefa não é executada estritamente dentro do cronograma, mas de forma aleatória dentro de um determinado intervalo, ou seja, os horários de início da tarefa são espalhados.
   - **Ligar dispositivos usando a função Wake-On-LAN antes de iniciar a tarefa**. Caso a caixa de seleção esteja marcada, o sistema operacional do computador receberá um tempo de espera especificado para concluir a inicialização antes que a tarefa seja executada. O de espera padrão é 5 minutos.
   - **Desligar os dispositivos após concluir a tarefa**. Caso a caixa de seleção esteja marcada, os dispositivos serão desligados após a conclusão da tarefa.
   - **Interromper a tarefa se ela durar mais do que**. Caso a caixa de seleção esteja marcada, a tarefa será interrompida se ela for executada por mais tempo do que o tempo especificado.
5. Clique no botão **Salvar** para salvar as configurações de início da tarefa.

Ativando e desativando tarefas programadas

É possível desativar as tarefas agendadas após definir as configurações de agendamento.

Para desativar o agendamento de inicialização da tarefa:

1. Na janela principal do Web Console, selecionar **Dispositivos** → **Tarefas**.
2. Clique no nome da tarefa na lista de tarefas do Kaspersky Security Center.

   A janela **<Nome da tarefa>** é exibida.
3. Ir para a seção **Configurações do aplicativo**.
4. Selecione a seção **Agendamento**.
5. Selecione as configurações para executar uma tarefa agendada a partir da lista suspensa **Início agendado** caso queira ativar o início da tarefa agendada.

6. Selecione **Manualmente** na lista suspensa caso queira desativar o início da tarefa agendada.

7. Clique no botão **Salvar**.

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:

- 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

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 para cada componente: *Em execução*, *Pausado*, *Interrompido*, *Não coberto pela licença*.

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 visualizar o status dos componentes no Kaspersky Security Center Web Console:

1. Na janela principal do Web Console, selecionar **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo e vá para a seção **Aplicativos**.
3. Clique no nome do aplicativo do Kaspersky Embedded Systems Security.

4. Na janela exibida, na guia **Geral**, clique na seção **Componentes**.

5. Revise a tabela de status.

Para analisar um relatório padrão no Kaspersky Security Center Web Console:

1. Selecione **Monitoramento e Relatórios → Relatórios**.

2. Selecione o item da lista **Relatório sobre o status dos componentes do aplicativo** e clique nele.

   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 Informar). 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 Ativa.

2. Selecione **Monitoramento e Relatórios → Relatórios**.

3. Selecione o item da lista **Relatório sobre os aplicativos proibidos no modo de teste** e clique nele.

   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 da lista **Relatório sobre aplicativos proibidos** e clique nele.

   Um relatório é gerado.

Este relatório contém os mesmos dados sobre blocos que o relatório de aplicativos proibidos no modo de teste.

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.
- Durante a instalação do Console do Kaspersky Embedded Systems Security.
- Lendo o documento do arquivo license.txt incluído no kit de distribuição.
- No site da Kaspersky (https://www.kaspersky.com/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.

Após a expiração da licença comercial, apenas os seguintes componentes e tarefas do aplicativo permanecem disponíveis sem atualizações do banco de dados:

- Proteção de Arquivos em Tempo Real
- Monitor de integridade do sistema
- Tarefas de Verificação por Demanda

Para continuar utilizando todos os recursos do Kaspersky Embedded Systems Security, é necessário renovar a licença comercial. É recomendável estender o período de validade da licença antes da data de expiração para garantir a proteção máxima.

Caso a chave de licença seja removida, o aplicativo continuará sendo executado. O componente Monitor de integridade do sistema permanece disponível, e o restante dos componentes, tarefas e atualizações do banco de dados do Kaspersky Embedded Systems Security ficam indisponíveis. O mesmo acontece se a Kaspersky adicionar sua licença na lista de permissões.

Sobre o certificado da licença

O *certificado de licença* é o documento fornecido junto com um arquivo de chave ou código de ativação.

O certificado de licença possui as seguintes informações sobre a licença fornecida:

- Identificador de licença ou número do pedido
- Informações sobre o usuário a quem foi concedida a licença
- Informações sobre o aplicativo que pode ser ativado com a licença fornecida
- A limitação no número de unidades licenciadas (por exemplo, o número de dispositivos nos quais o aplicativo pode ser usado mediante a licença)
- 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.

Há dois tipos de chaves: ativa e reserva.

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

Uma *chave reserva* é uma chave que confirma o direito de usar o aplicativo, mas que não está em uso. Uma chave reserva torna-se ativa automaticamente quando a licença associada à chave ativa atual expira. Uma chave reserva somente pode ser adicionada se a chave ativa estiver disponível.

Sobre o arquivo de chave

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

Você recebe um arquivo de chave no endereço de e-mail especificado após a compra do Kaspersky Embedded Systems Security.

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

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

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

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

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. Você recebe um código de ativação no endereço de e-mail especificado após a compra do Kaspersky Embedded Systems Security.

Para ativar o aplicativo utilizando o código de ativação, é necessário 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.

Comparação da funcionalidade do aplicativo dependendo do tipo de licença

O conjunto de funcionalidades do Kaspersky Embedded Systems Security depende do tipo de licença (consulte a tabela abaixo).

Comparação de recursos do Kaspersky Embedded Systems Security

Recurso	Kaspersky Embedded Systems Security	Kaspersky Embedded Systems Security Compliance Edition
Proteção de Arquivos em Tempo Real	✓	✓
Verificação por demanda	✓	✓
Controle de Inicialização de Aplicativos	✓	✓
Controle de dispositivos	✓	✓
Firewall	✓	✓
Monitor de Integridade de Arquivos	–	✓
Inspeção de log	–	✓

Ativar o aplicativo com um arquivo de chave

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

Para ativar o Kaspersky Embedded Systems Security com um arquivo de chave:

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

   Também é possível adicionar uma chave como chave reserva. Para adicionar uma chave adicional, marque a caixa de seleção **Usar como chave adicional**.

5. Clique **OK**.

O arquivo de chave selecionado será aplicado. Nesse caso:

- Se uma chave ativa já tiver sido adicionado para ativar o aplicativo e você adicionar outra chave como chave ativa, a nova chave substitui a adicionada anteriormente. A chave adicionada anteriormente é removida.
- Se uma chave reserva já tiver sido adicionada para ativar o aplicativo e outra for adicionada, a nova substituirá a anterior. A chave reserva adicionada anteriormente é removida.
- Se uma chave ativa e uma chave reserva já tiverem sido adicionadas para ativar o aplicativo e você adicionar uma nova chave como chave ativa, a nova chave substitui a chave ativa adicionada anteriormente; a chave reserva não é removida.

As informações sobre a chave adicionada estarão disponíveis no node **Licença**.

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 usando um código de ativação.

Com esse método, o Kaspersky Embedded Systems Security 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.
- 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 com um código de ativação por meio do Console do Aplicativo ou criando a tarefa de grupo *Ativação do aplicativo* por meio do plug-in de administração ou do plug-in da Web.

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

1. Na árvore do Console do Aplicativo, expanda o nó **Licença**.
2. Clique no link **Adicionar código de ativação** no painel de resultados do node **Licença**.
3. Na janela exibida, insira o código de ativação no campo **Código de ativação**.
   - Caso deseje usar o código de ativação como chave reserva, marque 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 **OK**.

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

Visualização das informações sobre a licença atual

Visualização do status da criptografia

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. O status da licença pode ter os seguintes valores:

- **Verificando o status da chave** – o Kaspersky Embedded Systems Security está verificando o arquivo de chave adicionado e está aguardando uma resposta sobre o status atual.
- **Data de expiração** – o Kaspersky Embedded Systems Security foi ativado até a data especificada. O status é realçado em amarelo nos seguintes casos:
  - A licença expira em 30 dias e nenhuma chave reserva foi adicionada.
  - A chave adicionada foi colocada na lista de bloqueio e está prestes a ser bloqueada.
- **O aplicativo não está ativado** – O Kaspersky Embedded Systems Security não foi ativado porque a chave não foi adicionada. O status é realçado em vermelho.
- **A licença expirou** – o Kaspersky Embedded Systems Security 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 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** – o arquivo de chave adicionado foi bloqueado e colocado na lista de bloqueio pela Kaspersky, por exemplo, se a chave foi usada 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 nó **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
Status do código de ativação ou da chave	Status do código de ativação ou da chave: *Chave ativa* ou *Chave Reserva*.
Data de expiração	Data e hora de expiração da licença associada a uma chave ativa.
Tipo de licença	Tipo de licença: *Licença comercial*.

Campo	Descrição
Status da ativação	As informações de status da ativação podem ter os seguintes valores: • **Aplicada** - se você ativou o aplicativo usando uma chave. • **Ativação do aplicativo** - 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	O número da chave usada para ativar o aplicativo.

Para visualizar informações detalhadas sobre a licença,

no painel de detalhes do nó **Licenciamento**, abra o menu de contexto da licença que deseja visualizar e selecione **Propriedades**.

Informações detalhadas sobre a licença na janela Propriedades <número da chave>

Campo	Descrição
Chave	O número da chave usada para ativar o aplicativo.
Aplicativo	O nome do aplicativo ativado com a chave adicionada.
Tipo de licença	Tipo de licença: comercial ou de avaliação.
Período da licença	O número de dias, contados a partir da data de ativação do aplicativo, durante os quais a licença é válida.
Data de ativação	Data em que a chave foi adicionada ao aplicativo.
Data de expiração	Data 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 não seja capaz de determinar a data de expiração da licença, o valor do campo é definido como *Desconhecido*.
Dias até a expiração	Número de dias restantes até a expiração da licença associada à chave ativa.
Elegível para suporte técnico	Informações sobre se a Kaspersky ou seus parceiros fornecerão suporte técnico aos clientes de acordo com os termos da licença.
Informações do Suporte	Detalhes de contato da Kaspersky ou de seu parceiro que fornece suporte técnico. Este campo pode ficar vazio se o suporte técnico não for fornecido.
Informações do proprietário	Informações sobre o cliente da licença: nome do cliente e da organização para os quais a licença foi adquirida.
Informações da licença	Número e tipo da licença atual.
Funcionalidade	Recursos do aplicativo disponíveis de acordo com a licença.

Renovação da licença

Por padrão, o Kaspersky Embedded Systems Security notifica o usuário quando restam 30 dias para a licença expirar.

É possível renovar a licença antes da data de expiração usando uma chave reserva. 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 **Licença**.

3. Execute uma das seguintes ações no painel de resultados do node **Licença**:

   - Se deseja renovar uma licença usando um arquivo de chave:

     a. Clique no link **Adicionar chave**.

     b. Clique no botão **Procurar** na janela que se abre.

     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 **OK**.

A chave reserva será adicionada e automaticamente aplicada após a expiração da licença atual do Kaspersky Embedded Systems Security.

Exclusão da chave

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

Para remover a chave adicionada anteriormente:

1. Na árvore do Console do Aplicativo, selecione o node **Licença**.
2. No painel de resultados do node **Licença**, 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.

Sobre a coleta de dados

O Contrato de Licença do Kaspersky Embedded Systems Security, 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, como parte do kit de distribuição e no menu **Iniciar** (**Todos os programas** > **Kaspersky Embedded Systems Security** > **EULA e Política de Privacidade**) após a instalação.

Durante a desinstalação do Kaspersky Embedded Systems Security, 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 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.

Área funcional	Registro de eventos
Tipo de uso	O Kaspersky Embedded Systems Security 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 Security for Windows Server\<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. Durante a desinstalação do Kaspersky Embedded Systems Security, todos os dados armazenados por ele no dispositivo protegido serão excluídos.
Finalidade	Fornecimento do recurso primário.

O Kaspersky Embedded Systems Security 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 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.
- 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. 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.

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

Área funcional	Todos os recursos do Kaspersky Embedded Systems Security
Tipo de uso	O Kaspersky Embedded Systems Security 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 Security for Windows Server\<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. Durante a desinstalação do Kaspersky Embedded Systems Security, todos os dados armazenados por ele no dispositivo protegido serão excluídos. O Kaspersky Embedded Systems Security não exclui os dados relacionados aos parâmetros exportados para o arquivo de configuração. O Kaspersky Embedded Systems Security não exclui objetos em Quarentena e 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 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 executa tarefas.
- Senha do Kaspersky Embedded Systems Security.
- 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.
- 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 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 permite configurar o nível de proteção para os dados processados localmente. 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 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 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 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 contém os componentes auxiliares do aplicativo, que podem ser instalados no dispositivo mesmo se o Kaspersky Embedded Systems Security 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, 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.

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 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 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; 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.

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

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

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

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

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

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 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 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 em dispositivos para os quais o envio de dados é proibido pela política da sua organização.

Por padrão, o Kaspersky Embedded Systems Security 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.

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 no dispositivo protegido.
- Informações sobre objetos processados pelo Kaspersky Endpoint Agent.
- Erros decorrentes durante a operação do Kaspersky Endpoint Agent.

Conformidade com a legislação da União Europeia (GDPR)

O Kaspersky Embedded Systems Security pode transmitir dados à Kaspersky quando:

- Usar a Kaspersky Security Network.
- Ativar o aplicativo com um código de ativação.
- Atualizar módulos de aplicativos e bancos de dados de antivírus.
- Acessar links no Console do Aplicativo.

Independentemente da classificação de dados e do território do qual os dados são recebidos, a Kaspersky segue altos padrões de segurança de dados e emprega várias medidas legais, organizacionais e técnicas para proteger os dados dos usuários, para garantir a segurança e confidencialidade dos dados e também para assegurar o cumprimento dos direitos dos usuários garantidos pela legislação aplicável. O texto da Política de Privacidade está incluso no kit de distribuição do aplicativo e está disponível no Site da Kaspersky.

Antes de usar o Kaspersky Embedded Systems Security, leia com atenção a descrição dos dados transmitidos no Contrato de Licença do Usuário Final e na Declaração da Kaspersky Security Network (listados na Declaração da Kaspersky Security Network). Se dados específicos transmitidos do Kaspersky Embedded Systems Security em qualquer um dos cenários descritos puderem ser classificados como dados pessoais de acordo com a legislação ou norma local, você deve garantir que tais dados sejam processados legalmente e obter o consentimento dos usuários finais para a coleta e transmissão desses dados.

Leia o Contrato de Licença do Usuário Final e visite o site da Kaspersky para saber mais sobre como recebemos, processamos, armazenamos e destruímos informações sobre o uso do aplicativo após você aceitar o Contrato de Licença do Usuário Final e concordar com a Declaração da Kaspersky Security Network. Os arquivos license.txt e ksn_<ID do idioma>.txt contêm o texto do Contrato de Licença de Usuário Final e a Declaração da Kaspersky Security Network e estão incluídos no kit de distribuição do aplicativo.

Se você não deseja transmitir dados à Kaspersky, pode desativar o fornecimento de dados.

Usando a Kaspersky Security Network

Ao usar a Kaspersky Security Network, você concorda em fornecer automaticamente os dados listados na Declaração da Kaspersky Security Network. Caso não concorde em fornecer esses dados à Kaspersky, use a Kaspersky Private Security Network (KPSN) ou desative o uso da KSN.

Ativação do aplicativo com um código

Ao usar um código de ativação, você concorda em fornecer automaticamente os dados no Contrato de Licença do Usuário Final. Se não concordar em fornecer esses dados à Kaspersky, use um arquivo de chave para ativar o Kaspersky Embedded Systems Security.

Atualizar módulos de aplicativos e bancos de dados de antivírus

Ao usar os servidores da Kaspersky, você concorda em fornecer automaticamente os dados no Contrato de Licença do Usuário Final. A Kaspersky requer essas informações para verificar se o Kaspersky Embedded Systems Security está sendo usado de forma legítima. Caso não concorde em fornecer essas informações à Kaspersky, use o Kaspersky Security Center para atualizações do banco de dados.

Acessar links no Console do Aplicativo.

Ao usar links no Console do aplicativo, você concorda em fornecer automaticamente os dados no Contrato de Licença do Usuário Final. A lista exata dos dados transmitidos em cada link específico depende de onde o link está localizado no Console do aplicativo e que problema ele visa resolver. Caso não concorde em fornecer essas informações à Kaspersky, desative a exibição da interface do aplicativo.

Inicialização e interrupção do Kaspersky Embedded Systems Security

Esta seção contém informações sobre como iniciar e interromper o Kaspersky Embedded Systems Security, além de informações sobre como iniciar o Kaspersky Embedded Systems Security Console e o plug-in de gerenciamento do Console de Administração do Kaspersky Security Center.

Iniciando e interrompendo o aplicativo

Depois de instalar o Kaspersky Embedded Systems Security no computador de um usuário, o aplicativo é iniciado automaticamente. Por padrão, o Kaspersky Embedded Systems Security é iniciado depois da inicialização do sistema operacional. Não é possível configurar a inicialização automática do aplicativo nas configurações do sistema operacional.

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

Como configurar a inicialização automática do aplicativo no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações do aplicativo** → **Segurança e confiabilidade** e clique em **Configurações**.
4. Na guia **Segurança**, marque ou desmarque a caixa de seleção **Iniciar o aplicativo na inicialização do computador (recomendado)** para ativar ou desativar a execução automática do aplicativo.
5. Salvar alterações.

Como configurar a inicialização automática do aplicativo no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.

4. Selecione **Configurações do aplicativo → Segurança e confiabilidade**.
5. Clique **Configurar**.

   A janela **Segurança e confiabilidade** é aberta.
6. Use a caixa de seleção **Iniciar o aplicativo na inicialização do computador (recomendado)** para ativar ou desativar a inicialização automática do aplicativo.
7. Salvar alterações.

Como configurar a inicialização automática do aplicativo no Console do Aplicativo

1. selecione o nó **Kaspersky Embedded Systems Security** na árvore do Console do Aplicativo.
2. Selecione **Propriedades do aplicativo** no menu de contexto do node.
3. Uma janela será aberta; nessa janela, selecione a guia **Configurações de segurança**.
4. Use a caixa de seleção **Iniciar o aplicativo na inicialização do computador (recomendado)** para ativar ou desativar a inicialização automática do aplicativo.
5. Salvar alterações.

Você pode iniciar e interromper o Kaspersky Embedded Systems Security se for membro do grupo de Administradores no dispositivo protegido.

Como iniciar ou interromper o aplicativo no Console de Administração do Kaspersky Security Center

1. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.
2. No espaço de trabalho, selecione a guia **Dispositivos**.
3. Clique duas vezes para abrir a janela de propriedades do computador.
4. Na janela de propriedades do computador, selecione a seção **Aplicativos**.
5. Na lista de aplicativos da Kaspersky instalados no computador, selecione **Kaspersky Embedded Systems Security for Windows (4.0.0)**.
6. Execute uma das seguintes ações:

   - Para iniciar o aplicativo, clique no botão à direita da lista de aplicativos da Kaspersky.
   - Para encerrar o aplicativo, clique no botão à direita da lista de aplicativos da Kaspersky.

Como iniciar ou interromper o aplicativo no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Dispositivos gerenciados**.
2. Clique no nome do computador no qual você quer iniciar ou interromper o Kaspersky Embedded Systems Security.

   A janela de propriedades do computador é exibida.
3. Selecione a guia **Aplicativos**.
4. Marque a caixa de seleção ao lado de **Kaspersky Embedded Systems Security for Windows (4.0.0)**.
5. Clique nos botões **Iniciar** ou **Parar**.

Como iniciar ou interromper o aplicativo no Console do Aplicativo

1. Na árvore do Console do Aplicativo, na área de trabalho do nó **Kaspersky Embedded Systems Security**, clique em **Conectar a um computador remoto**.
2. Na mensagem de reinicialização do aplicativo, clique em **Sim**.
3. Na janela **Selecionar o dispositivo protegido**, ao lado de **Gerenciando o serviço**, execute uma das seguintes ações:
   - Caso queira interromper o aplicativo, clique no botão **Interromper**.
   - Caso queira iniciar o aplicativo, clique no botão **Iniciar**.

O aplicativo será interrompido ou iniciado.

A janela **Selecionar o dispositivo protegido** também será exibida se a conexão com o computador no qual o aplicativo está instalado for perdida ou se o serviço KESS apresentar falhas. É possível restaurar o serviço KESS clicando no botão **Iniciar**.

Como iniciar ou interromper o aplicativo na linha de comando

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.
2. Usando o comando `cd` , navegue até a pasta onde os arquivos klpsm.exe e kavshell.exe estão localizados.

   Por exemplo, `cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0`

3. Para iniciar o aplicativo por meio da linha de comando, execute um dos seguintes comandos:

   - `klpsm.exe start_avp_service`
   - `KAVSHELL start [/login:<nome da conta de usuário atual>] [/PWD:<senha de /login ou senha do KLAdmin caso /login não seja especificado>]`

4. Para interromper o aplicativo por meio da linha de comando, execute um dos seguintes comandos:

   - `klpsm.exe stop_avp_service`
   - `KAVSHELL stop [/login:<nome da conta de usuário atual>] [/PWD:<senha de /login ou senha do KLAdmin caso /login não seja especificado>]`

Pausar e reiniciar a Proteção e Controle do computador

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

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

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

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

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

Para pausar a Proteção e Controle do computador:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.
2. Selecione **Pausar a proteção**.
3. Selecione uma das seguintes opções:

   - **Pausar pelo tempo especificado <intervalo de tempo>** – a proteção e o controle do computador serão reiniciados após decorrer o tempo especificado na lista suspensa abaixo.
   - **Pausar até reiniciar**– A Proteção e Controle do computador continuarão após você reabrir o aplicativo ou reiniciar o sistema operacional. A inicialização automática do aplicativo precisa ser ativada para que esta opção possa ser usada.
   - **Pausar** – A Proteção e Controle do computador continuarão quando você decidir reativá-los.

O Kaspersky Embedded Systems Security pausará a operação de proteção e controle de todos os componentes que não estiverem bloqueados () na política.

Para reiniciar a proteção e controle do computador:

1. Abra o menu de contexto do ícone do aplicativo, localizado na área de notificação da barra de tarefas.

2. No menu de contexto, selecione **Reiniciar a proteção**.

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

Interface de diagnóstico compacta

Esta seção descreve o uso da Interface Compacta de Diagnóstico.

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 avpui.exe na pasta do aplicativo no dispositivo protegido.

Na Interface de Diagnóstico Compacta é possível fazer o seguinte:

- Abrir a janela **Sobre** com a lista de atualizações instaladas e patches disponíveis.
- 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.

A Interface de Diagnóstico Compacta está disponível mesmo se o acesso às funções do Kaspersky Embedded Systems Security 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 por meio da Interface de diagnóstico compacta

Para analisar o status do aplicativo por meio da Interface de diagnóstico compacta:

1. Abra a Interface Compacta de Diagnóstico da seguinte maneira:
   - Execute o arquivo avpui.exe na pasta de instalação do aplicativo no dispositivo protegido. Por padrão, o arquivo está localizado em C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0.
   - Clique no ícone de aplicativo na área de notificação da área de tarefas.

2. Revise o status atual da chave, as tarefas de Proteção do Computador em Tempo Real e as tarefas de Atualização na seção **Status de proteção**. As cores diferentes são usadas para notificar o usuário sobre o status de proteção (ver a tabela abaixo).

Indicação de cor na janela da Interface Compacta de Diagnóstico

Seção	Status

Status da 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 **Bloquear** 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 **Informar**. • A Prevenção de Exploits e a tarefa de Controle de Inicialização de Aplicativos são iniciadas no modo **Informar**.
	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 **Informar**.
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 30 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: • *O aplicativo não está ativado.* • *A licença expirou.* • *O Contrato de Licença do Usuário Final foi violado.* • *A chave está na lista de bloqueio.*
Atualizar	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 seção **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 exibir as estatísticas:

1. Abra a Interface Compacta de Diagnóstico da seguinte maneira:
   - Execute o arquivo avpui.exe na pasta de instalação do aplicativo no dispositivo protegido. Por padrão, o arquivo está localizado em C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0.
   - Clique no ícone de aplicativo na área de notificação da área de tarefas.
2. Ir para a seção **Estatísticas**.
3. Revise os incidentes de segurança para as tarefas de proteção.

Revisando a atividade atual do aplicativo

Para revisar a atividade atual do aplicativo no dispositivo protegido:

1. Abra a Interface Compacta de Diagnóstico da seguinte maneira:
   - Execute o arquivo avpui.exe na pasta de instalação do aplicativo no dispositivo protegido. Por padrão, o arquivo está localizado em C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0.
   - Clique no ícone de aplicativo na área de notificação da área de tarefas.
2. Ir para a seção **Atividade atual dos aplicativos**.

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 **Uso da KSN** é iniciada.
  - *Amarelo*. A Declaração da KSN é aceita, mas a tarefa não é iniciada.

Configurando o rastreamento do aplicativo e registro do despejo de memória

Para configurar o rastreamento do aplicativo e registro do despejo de memória:

1. Abra a Interface Compacta de Diagnóstico da seguinte maneira:

   - Execute o arquivo avpui.exe na pasta de instalação do aplicativo no dispositivo protegido. Por padrão, o arquivo está localizado em C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0.

   - Clique no ícone de aplicativo na área de notificação da área de tarefas.

2. Ir para a seção **Diagnóstico de mau funcionamento**.

3. Use a caixa de seleção **Gravar as informações de depuração no arquivo de rastreamento** para ativar ou desativar o rastreamento de operação do aplicativo.

4. Caso seja necessário, clique no botão **Procurar** para especificar a pasta na qual o Kaspersky Embedded Systems Security 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. Na lista suspensa **Nível de detalhes**, selecione o nível de detalhes das informações de depuração.

   - **Crítico** significa que o arquivo de rastreamento salva apenas as mensagens referentes aos erros fatais.

   - **Diagnóstico** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros e avisos.

   - **Importante** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros, avisos e informações adicionais.

   - **Normal** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros e avisos, além das informações sobre a operação normal do aplicativo (padrão).

   - **Detalhado** significa que o arquivo de rastreamento salva todas as informações referentes à operação do aplicativo.

   Um representante do Suporte Técnico determina o nível de detalhe necessário para solucionar qualquer problema que venha a ocorrer.

   O nível de detalhes padrão é configurado como **Normal**.

6. Especifique o **Tamanho máximo de um arquivo de rastreamento (MB)**.

   Valores disponíveis: de 1 a 4095 MB. Por padrão, o tamanho máximo dos arquivos de rastreamento é definido como 100 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 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. Caso seja necessário, configure os despejos de memória:

   a. Marque ou desmarque a caixa de seleção **Criar arquivo de despejo sobre funcionamento incorreto na pasta** para ativar ou desativar o despejo de memória em caso de funcionamento incorreto.

   b. Caso seja necessário, clique no botão **Procurar** para especificar a pasta na qual o Kaspersky Embedded Systems Security salvará os arquivos de despejo da memória. Por padrão, os arquivos de despejos de memória são armazenados na seguinte pasta: %ProgramData%\Kaspersky Lab\KESS.4.0\Traces.

   > 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.

10. Clique **Aplicar**.

Autodefesa do Kaspersky Embedded Systems Security

A Autodefesa evita que outros aplicativos executem ações que possam interferir na operação do Kaspersky Embedded Systems Security. O aplicativo tem mecanismos de autodefesa que o protegem contra a modificação ou exclusão de suas pastas, processos da memória e entradas no registro do sistema. O Kaspersky Embedded Systems Security é compatível com a tecnologia Antimalware Protected Process Light (AM-PPL) da Microsoft, que protege os processos do aplicativo contra atividades maliciosas. Além disso, o aplicativo permite gerenciar as permissões de acesso do usuário à funcionalidade do aplicativo separadamente do serviço do aplicativo.

Ativar ou desativar a Autodefesa

O Kaspersky Embedded Systems Security impede que haja alteração ou exclusão de arquivos de aplicativo no disco rígido, processos na memória e entradas no registro do sistema.

A tecnologia bloqueia o acesso aos seguintes componentes do aplicativo:

- arquivos na pasta de instalação do Kaspersky Embedded Systems Security e outros arquivos do aplicativo;
- chaves de registro com registros pertencentes ao aplicativo;
- processos que o aplicativo executa.

Os mecanismos de Autodefesa do Kaspersky Embedded Systems Security são ativados por padrão.

Como ativar ou desativar a Autodefesa no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de propriedades da política, acesse a seção **Configurações do aplicativo**.
4. No bloco **Segurança e confiabilidade**, clique no botão **Configurações**.
5. Uma janela será aberta; nessa janela, selecione a guia **Segurança**.
6. No bloco **Autodefesa**, use a caixa de seleção **Proteger os processos do aplicativo contra ameaças externas** para ativar ou desativar a Autodefesa.
7. Feche o cadeado para aplicar a política aos computadores.
8. Clique no botão **OK** para salvar as alterações.

Como ativar ou desativar a Autodefesa no Console do aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e no painel de resultados, siga o link **Propriedades do aplicativo**.
2. Uma janela será aberta; nessa janela, selecione a guia **Configurações de segurança**.
3. No bloco **Autodefesa**, use a caixa de seleção **Proteger os processos do aplicativo contra ameaças externas** para ativar ou desativar a Autodefesa.
4. Clique no botão **OK** para salvar as alterações.

Como ativar ou desativar a Autodefesa no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Configurações do aplicativo**.
5. No bloco **Segurança e confiabilidade**, clique no botão **Configurar**.

   A janela **Segurança e confiabilidade** é aberta.
6. No bloco **Autodefesa**, use a caixa de seleção **Proteger os processos do aplicativo contra ameaças externas** para ativar ou desativar a Autodefesa.
7. Feche o cadeado para aplicar a política aos computadores.
8. Clique no botão **OK** para salvar as alterações.

Compatibilidade com a tecnologia AM-PPL

O Kaspersky Embedded Systems Security é compatível com a tecnologia Antimalware Protected Process Light (doravante denominada "AM-PPL") da Microsoft. O AM-PPL protege os processos do Kaspersky Embedded Systems Security contra ações maliciosas (por exemplo, encerrando o aplicativo). O AM-PPL permite que apenas processos confiáveis sejam executados. Os processos do Kaspersky Embedded Systems Security são assinados de acordo com os requisitos de segurança do Windows e, portanto, são confiáveis. Para obter mais detalhes sobre a tecnologia AM-PPL, visite o site da Microsoft. A tecnologia AM-PPL está ativada por padrão.

O Kaspersky Embedded Systems Security também possui mecanismos internos para proteger os processos do aplicativo. O suporte ao AM-PPL permite delegar funções de segurança do processo ao sistema operacional. Dessa forma, você pode aumentar a velocidade do aplicativo e reduzir o consumo de recursos do computador.

O aplicativo registra o serviço Kaspersky Embedded Systems Security (AVP) e o serviço Kaspersky Seamless Update Service (AVPSUS). A tecnologia AM-PPL protege apenas o serviço AVP.

Mantenha a tecnologia AM-PPL sempre ativa. O AM-PPL é um componente importante de defesa do sistema operacional. É permitido desativar AM-PPL somente em um ambiente de teste separado com a finalidade de solucionar problemas do aplicativo.

A tecnologia AM-PPL está disponível para os sistemas operacionais Windows 10 versão 1703 (RS2) ou posterior e Windows Server 2019.

Para ativar ou desativar a tecnologia AM-PPL:

1. Desative o mecanismo de autodefesa do aplicativo.

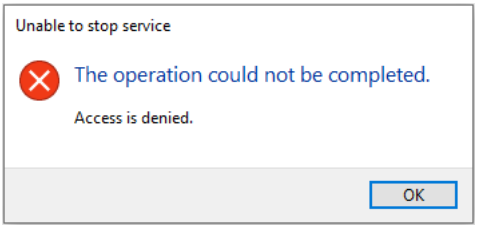
   O mecanismo de autodefesa impede a modificação e a exclusão dos processos de aplicativos na memória do computador, incluindo a alteração do status do AM-PPL.

2. Execute o interpretador da linha de comando (cmd) como um administrador.
3. Vá até a pasta onde o arquivo executável do Kaspersky Embedded Systems Security está localizado.
4. Digite o seguinte na linha de comando:

   - `klpsm.exe enable` – ativação do suporte à tecnologia AM-PPL.
   - `klpsm.exe disable` – desativa o suporte à tecnologia AM-PPL.

5. Reinicie o Kaspersky Embedded Systems Security.
6. Continuar com o mecanismo de autodefesa do aplicativo.

Assim, quando um usuário tentar interromper o serviço AVP, aparecerá uma janela do sistema com uma mensagem de erro. O usuário só poderá gerenciar os serviços do aplicativo por meio da interface do Kaspersky Embedded Systems Security.



Erro de acesso aos serviços do aplicativo

Proteção de serviços do sistema operacional

A funcionalidade *Proteger serviços do sistema operacional* pode ser usada para permitir ou proibir aplicativos de terceiros de atuar nos serviços do sistema operacional.

Como ativar ou desativar a proteção dos serviços do sistema operacional no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de propriedades da política, acesse a seção **Configurações do aplicativo**.
4. No bloco **Segurança e confiabilidade**, clique no botão **Configurações**.
5. Uma janela será aberta; nessa janela, selecione a guia **Segurança**.
6. Use a caixa de seleção **Proteger serviços do sistema operacional** para ativar ou desativar a proteção dos serviços do sistema operacional.

   Se a proteção dos serviços do sistema operacional estiver ativada, os aplicativos de terceiros não podem agir sobre os processos do sistema operacional.

   Se a proteção dos serviços do sistema operacional estiver desativada, os aplicativos de terceiros podem agir sobre os processos do sistema operacional.

   Você deve reiniciar o computador após ativar ou desativar a função para aplicar as alterações.
7. Feche o cadeado para aplicar a política aos computadores.
8. Clique no botão **OK** para salvar as alterações.

Como ativar ou desativar a proteção dos serviços do sistema operacional no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e no painel de resultados, siga o link **Propriedades do aplicativo**.
2. Uma janela será aberta; nessa janela, selecione a guia **Configurações de segurança**.
3. Use a caixa de seleção **Proteger serviços do sistema operacional** para ativar ou desativar a proteção dos serviços do sistema operacional.

   Se a proteção dos serviços do sistema operacional estiver ativada, os aplicativos de terceiros não podem agir sobre os processos do sistema operacional.

   Se a proteção dos serviços do sistema operacional estiver desativada, os aplicativos de terceiros podem agir sobre os processos do sistema operacional.

   Você deve reiniciar o computador após ativar ou desativar a função para aplicar as alterações.
4. Clique no botão **OK** para salvar as alterações.

Como ativar ou desativar a proteção dos serviços do sistema operacional no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Configurações do aplicativo**.
5. No bloco **Segurança e confiabilidade**, clique no botão **Configurar**.

   A janela **Segurança e confiabilidade** é aberta.
6. Use a caixa de seleção **Proteger serviços do sistema operacional** para ativar ou desativar a proteção dos serviços do sistema operacional.

   Se a proteção dos serviços do sistema operacional estiver ativada, os aplicativos de terceiros não podem agir sobre os processos do sistema operacional.

   Se a proteção dos serviços do sistema operacional estiver desativada, os aplicativos de terceiros podem agir sobre os processos do sistema operacional.

   Você deve reiniciar o computador após ativar ou desativar a função para aplicar as alterações.
7. Feche o cadeado para aplicar a política aos computadores.
8. Clique no botão **OK** para salvar as alterações.

Configuração de permissões de usuário para gerenciar o Kaspersky Embedded Systems Security

Por padrão, todos os recursos do Kaspersky Embedded Systems Security podem ser acessados por membros do grupo Administradores no dispositivo protegido, membros do grupo Administradores de ESS, criado no dispositivo protegido durante a instalação do Kaspersky Embedded Systems Security, e pelo grupo SYSTEM.

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

É possível permitir ou bloquear o acesso a funções específicas do Kaspersky Embedded Systems Security para usuários específicos ou grupos de usuários.

Sobre permissões de acesso para funções do Kaspersky Embedded Systems Security

Direitos de usuário	Descrição
Gerenciar tarefas	Capacidade para iniciar/parar/pausar/reiniciar tarefas do Kaspersky Embedded Systems Security.
Criar e remover tarefas	Capacidade para criar e excluir tarefas de Verificação por Demanda.
Editar configurações	Capacidade para: • Importar as configurações do Kaspersky Embedded Systems Security a partir de um arquivo de configuração. • Editar as configurações do aplicativo.

Direitos de usuário	Descrição
Ler configurações	Capacidade para: • Visualizar as configurações gerais e configurações de tarefas do Kaspersky Embedded Systems Security. • Exportar as configurações do Kaspersky Embedded Systems Security 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 registros	Capacidade para excluir logs de tarefas e limpar o log de auditoria do sistema.
Ler registros	Capacidade para visualizar eventos do Antivírus em logs de tarefas e no log de auditoria do sistema.
Recuperar estatísticas	Capacidade de visualizar estatísticas de cada tarefa do Kaspersky Embedded Systems Security.
Gerenciar licenças do aplicativo	Capacidade de ativar o Kaspersky Embedded Systems Security.
Desinstalar o aplicativo	Capacidade de desinstalar o Kaspersky Embedded Systems Security.
Ler permissões	Capacidade de visualizar a lista de usuários do Kaspersky Embedded Systems Security e privilégios de acesso dos usuários.
Editar permissões	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.
Conexão remota com o aplicativo	Capacidade de se conectar remotamente ao aplicativo usando o Console do aplicativo. Para acesso remoto, o usuário também deve ter os direitos de acesso à funcionalidade **Ler configurações** .
Sair do aplicativo	Capacidade de sair do aplicativo usando o Console do aplicativo.
Desativar política do Kaspersky Security Center	Capacidade desativar a política do Kaspersky Security Center.
Exportar configurações	Capacidade de exportar as configurações do Kaspersky Embedded Systems Security.

Como configurar permissões de usuário para gerenciamento do Kaspersky Embedded Systems Security no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Suplementar**.
4. Na seção **Permissões de acesso do usuário para gerenciamento do aplicativo**, clique no botão **Configurações**.
5. Essa ação abrirá uma janela. Nessa janela, marque a caixa de seleção **Permitir confirmação de ações com o aplicativo usando credenciais de usuários criadas manualmente** e defina uma senha para a conta KLAdmin. A conta de usuário será automaticamente adicionada na lista de contas de usuário.
6. Caso seja necessário, adicione as contas de usuário às quais deseja conceder acesso ao gerenciamento de aplicativos. Para isso, clique em **Adicionar** na tabela de contas de usuário.

   Isso abre o formulário para configurar as permissões de acesso do usuário.

7. Selecione o método que deseja usar para adicionar usuários:

   - **Selecionar um usuário/grupo do Active Directory**. É possível conceder o acesso do Kaspersky Embedded Systems Security a usuários individuais ou grupos dentro do domínio do Active Directory. Por exemplo, se a opção de sair do aplicativo estiver bloqueada para o grupo Todos, você poderá conceder a permissão **Sair do aplicativo** para um usuário individual.

   - **Adicionar um usuário/grupo de usuários o manualmente**. É possível criar uma conta de usuário que não está presente no Active Directory e atribuir permissões individuais para essa conta. Ou seja, é possível criar uma *conta de usuário do serviço* e usá-la em vez do KLAdmin. Assim, não é necessário compartilhar sua senha do KLAdmin com outros usuários ou criar novas contas de usuário do Active Directory. É possível especificar qualquer nome de usuário e senha. Por exemplo, é possível conceder a permissão **Ler registros** para a conta de usuário do serviço. Como resultado, caso a visualização de relatórios esteja proibida para o grupo "Todos", é possível abrir os relatórios usando a conta de usuário do serviço ou pela conta de usuário do KLAdmin.

     Para adicionar um usuário ou grupo de usuários manualmente, é necessário ativar a Proteção por senha.

8. Selecione um usuário ou grupo de usuários para os quais deseja conceder acesso ao gerenciamento do aplicativo.

9. Na lista **Permissões**, configure as permissões de acesso do usuário à funcionalidade do aplicativo.

10. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como configurar permissões de usuário para gerenciamento do Kaspersky Embedded Systems Security no Console do aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e selecione **Permissões de acesso do usuário para gerenciamento do aplicativo** por meio do menu de contexto do nó.

2. Essa ação abrirá uma janela. Nessa janela, marque a caixa de seleção **Permitir confirmação de ações com o aplicativo usando credenciais de usuários criadas manualmente** e defina uma senha para a conta KLAdmin. A conta de usuário será automaticamente adicionada na lista de contas de usuário.

3. Caso seja necessário, adicione as contas de usuário às quais deseja conceder acesso ao gerenciamento de aplicativos. Para isso, clique em **Adicionar** na tabela de contas de usuário.

   Isso abre o formulário para configurar as permissões de acesso do usuário.

4. Selecione o método que deseja usar para adicionar usuários:

   - **Selecionar um usuário/grupo do Active Directory**. É possível conceder o acesso do Kaspersky Embedded Systems Security a usuários individuais ou grupos dentro do domínio do Active Directory. Por exemplo, se a opção de sair do aplicativo estiver bloqueada para o grupo Todos, você poderá conceder a permissão **Sair do aplicativo** para um usuário individual.

   - **Adicionar um usuário/grupo de usuários o manualmente**. É possível criar uma conta de usuário que não está presente no Active Directory e atribuir permissões individuais para essa conta. Ou seja, é possível criar uma *conta de usuário do serviço* e usá-la em vez do KLAdmin. Assim, não é necessário compartilhar sua senha do KLAdmin com outros usuários ou criar novas contas de usuário do Active Directory. É possível especificar qualquer nome de usuário e senha. Por exemplo, é possível conceder a permissão **Ler registros** para a conta de usuário do serviço. Como resultado, caso a visualização de relatórios esteja proibida para o grupo "Todos", é possível abrir os relatórios usando a conta de usuário do serviço ou pela conta de usuário do KLAdmin.

     Para adicionar um usuário ou grupo de usuários manualmente, é necessário ativar a Proteção por senha.

5. Selecione um usuário ou grupo de usuários para os quais deseja conceder acesso ao gerenciamento do aplicativo.

6. Na lista **Permissões**, configure as permissões de acesso do usuário à funcionalidade do aplicativo.

7. Salvar alterações.

Como configurar os direitos de acesso do usuário para gerenciamento do Kaspersky Embedded Systems Security no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Vá para **Suplementar** → **Permissões de acesso do usuário para gerenciamento do aplicativo** e clique no botão **Configurar**.

5. Essa ação abrirá uma janela. Nessa janela, marque a caixa de seleção **Permitir confirmação de ações com o aplicativo usando credenciais de usuários criadas manualmente** e defina uma senha para a conta KLAdmin. A conta de usuário será automaticamente adicionada na lista de contas de usuário.

6. Caso seja necessário, adicione as contas de usuário às quais deseja conceder acesso ao gerenciamento de aplicativos. Para isso, clique em **Adicionar** na tabela de contas de usuário.

   Isso abre o formulário para configurar as permissões de acesso do usuário.

7. Selecione o método que deseja usar para adicionar usuários:

   - **Selecionar um usuário/grupo do Active Directory**. É possível conceder o acesso do Kaspersky Embedded Systems Security a usuários individuais ou grupos dentro do domínio do Active Directory. Por exemplo, se a opção de sair do aplicativo estiver bloqueada para o grupo Todos, você poderá conceder a permissão **Sair do aplicativo** para um usuário individual.

   - **Adicionar um usuário/grupo de usuários o manualmente**. É possível criar uma conta de usuário que não está presente no Active Directory e atribuir permissões individuais para essa conta. Ou seja, é possível criar uma *conta de usuário do serviço* e usá-la em vez do KLAdmin. Assim, não é necessário compartilhar sua senha do KLAdmin com outros usuários ou criar novas contas de usuário do Active Directory. É possível especificar qualquer nome de usuário e senha. Por exemplo, é possível conceder a permissão **Ler registros** para a conta de usuário do serviço. Como resultado, caso a visualização de relatórios esteja proibida para o grupo "Todos", é possível abrir os relatórios usando a conta de usuário do serviço ou pela conta de usuário do KLAdmin.

     Para adicionar um usuário ou grupo de usuários manualmente, é necessário ativar a Proteção por senha.

8. Selecione um usuário ou grupo de usuários para os quais deseja conceder acesso ao gerenciamento do aplicativo.

9. Na lista **Permissões**, configure as permissões de acesso do usuário à funcionalidade do aplicativo.

10. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Configuração de permissões de acesso de usuários para gerenciar o Kaspersky Security Service

Durante a instalação, o Kaspersky Embedded Systems Security registra o serviço do aplicativo, *Kaspersky Security Service*, no Windows. Assim, o aplicativo inclui componentes funcionais que são inicializados ao iniciar o sistema operacional. Para reduzir o risco de acesso de terceiros à funcionalidade do aplicativo e às configurações de segurança do dispositivo protegido usando o serviço do aplicativo, é possível restringir as permissões de gerenciamento do 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. 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.

Usuários com acesso às funções do nível de permissões Editar podem conceder permissões de acesso para gerenciamento do 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 para gerenciar o Kaspersky Security Service:

- **Controle total**: capacidade de visualizar e editar configurações gerais e permissões de usuário do 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.
- **Editar**: capacidade de visualizar e editar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
- **Executar**: 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 (consulte a tabela abaixo).

Permissões de acesso para as funções do Kaspersky Security Service

Recurso	Descrição
Ler as configurações de serviço	Capacidade de visualizar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
Solicitar status de serviço do Service Control Manager	Capacidade de solicitar o status de execução do Kaspersky Security Service pelo Gerenciador de Controle de Serviço do Microsoft Windows.
Solicitar status do 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.
Modificar configurações do serviço	Capacidade de visualizar e editar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
Iniciar serviço	Capacidade de iniciar o Kaspersky Security Service.
Parar serviço	Capacidade de interromper o Kaspersky Security Service.
Pausar/retomar serviço	Capacidade de pausar e reiniciar o Kaspersky Security Service.
Ler permissões	Capacidade de visualizar a lista de usuários do Kaspersky Security Service e os privilégios de acesso de cada usuário.
Editar permissões	Capacidade para: • Adicionar e remover usuários do Kaspersky Security Service. • Editar permissões de acesso de usuários ao Kaspersky Security Service.
Remover serviço	Capacidade de anular o registro do Kaspersky Security Service no Gerenciador de Controle de Serviço do Microsoft Windows.
Solicitações de serviço definidos pelo usuário	Capacidade de criar e enviar solicitações de usuário ao Kaspersky Security Service.

É possível editar a lista de usuários e grupos de usuários com permissão para gerenciar o Kaspersky Security Service, bem como editar as permissões de acesso desses usuários e grupos de usuários.

Como configurar as permissões de usuário para gerenciamento do Kaspersky Security Service no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Suplementar**.

4. Na seção **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service**, clique no botão **Configurações**.

   Isso abre o formulário para configurar as permissões de acesso do usuário.

5. Adicione um usuário ou grupo do Active Directory para configurar suas respectivas permissões de usuário do Kaspersky Security Service.

6. Selecione um usuário ou grupo de usuários para os quais deseja conceder acesso ao gerenciamento do aplicativo.

7. Na lista de permissões, configure as permissões de usuário para gerenciar o Kaspersky Security Service.

8. Se necessário, configure permissões especiais para usuários:

   a. Clique em **Adicional**.

   b. Isso abre uma janela; nessa janela selecione uma conta de usuário.

   c. Clique duas vezes para abrir as propriedades da conta de usuário.

   d. Isso abre uma janela; nessa janela, clique no link **Mostrar permissões adicionais**.

   e. Isso abre uma janela; nessa janela, configure permissões especiais para o usuário.

9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como configurar as permissões de usuário para gerenciamento do Kaspersky Security Service no Console do aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e selecione **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service** por meio do menu de contexto do nó.

2. Na janela exibida, no bloco **Permissões**, clique no botão **Adicionar**.

   Isso abre o formulário para configurar as permissões de acesso do usuário.

3. Adicione um usuário ou grupo do Active Directory para configurar suas respectivas permissões de usuário do Kaspersky Security Service.

4. Selecione um usuário ou grupo de usuários para os quais deseja conceder acesso ao gerenciamento do aplicativo.

5. Na lista de permissões, configure as permissões de usuário para gerenciar o Kaspersky Security Service.

6. Se necessário, configure permissões especiais para usuários:

   a. Clique em **Adicional**.

   b. Isso abre uma janela; nessa janela selecione uma conta de usuário.

   c. Clique duas vezes para abrir as propriedades da conta de usuário.

d. Isso abre uma janela; nessa janela, clique no link **Mostrar permissões adicionais**.

e. Isso abre uma janela; nessa janela, configure permissões especiais para o usuário.

7. Salvar alterações.

Como configurar as permissões de usuário para gerenciamento do Kaspersky Security Service no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Suplementar** → **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service** e clique no botão **Configurar**.

   A janela **Permissões de acesso do usuário para o gerenciamento do Kaspersky Security Service** é aberta.
5. Adicione um usuário ou grupo do Active Directory para configurar suas respectivas permissões de usuário do Kaspersky Security Service.
6. Selecione um usuário ou grupo de usuários para os quais deseja conceder acesso ao gerenciamento do aplicativo.

   Não é possível configurar permissões especiais para gerenciamento do serviço do aplicativo no Web Console.
7. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Acesso protegido por senha às funções do Kaspersky Embedded Systems Security

Configurar direitos de usuário permite restringir o acesso ao gerenciamento do aplicativo e a serviços registrados configurando permissões de usuário. Também é possível estabelecer uma proteção por senha nas configurações do Kaspersky Embedded Systems Security para proteção adicional de operações críticas.

Quando um usuário tenta executar uma ação protegida por senha, o Kaspersky Embedded Systems Security solicita o nome de usuário e a senha ou a senha temporária. A proteção por senha suporta as seguintes contas:

- **KLAdmin**. Uma conta de administrador com acesso irrestrito ao Kaspersky Embedded Systems Security. A conta KLAdmin tem o direito de executar qualquer ação protegida por senha. As permissões para a conta KLAdmin não podem ser revogadas. Quando você ativa a proteção por senha, o Kaspersky Embedded Systems Security solicita que você defina uma senha para a conta do KLAdmin.

- **Conta adicionada manualmente**. Uma conta fora do domínio do Active Directory. É possível usar essa conta do serviço em vez do KLAdmin caso não deseje compartilhar a senha do administrador. É possível definir qualquer nome de usuário e senha e configurar permissões individuais.

- **O grupo Todos**. Um grupo interno do Windows que inclui todos os usuários dentro da rede corporativa. Os usuários do grupo Todos podem acessar o aplicativo de acordo com as permissões concedidas a eles.

- **Usuários individuais ou grupos**. Contas de usuário para as quais você pode configurar permissões individuais. Por exemplo, se uma ação for bloqueada para o grupo Todos, você poderá permitir essa ação para um usuário individual ou um grupo.

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

O Kaspersky Embedded Systems Security 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 maiúsculas latinas (A-Z)
  - Letras minúsculas latinas (a-z)
  - Números (0-9)
  - Ponto de exclamação (!), cifrão ($), cerquilha (#) e sinal de porcentagem (%)

Como proteger com senha o acesso à funcionalidade do Kaspersky Embedded Systems Security no Console de administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Suplementar**.
4. Na seção **Permissões de acesso do usuário para gerenciamento do aplicativo**, clique no botão **Configurações**.

5. Na janela que é aberta, marque a caixa de seleção **Permitir confirmação de ações com o aplicativo usando credenciais de usuários criadas manualmente**.

6. Caso seja necessário, desmarque a caixa de seleção **Solicitar senha para confirmar ações críticas**.

   Caso esta funcionalidade esteja ativada, o aplicativo solicitará um nome de usuário e senha ao excluir, modificar ou recuperar o aplicativo e ao executar **ações na linha de comando que possam diminuir o nível de proteção do dispositivo.**

   O aplicativo solicita credenciais ao executar os seguintes comandos:

   - `KAVSHELL APPCONTROL`
   - `KAVSHELL APPCONTROL /CONFIG`
   - `KAVSHELL APPCONTROL /GENERATE /import`
   - `KAVSHELL DEVCONTROL`
   - `KAVSHELL EXITPOLICY`
   - `KAVSHELL IMPORT`
   - `KAVSHELL ISOLATION /DISABLE`
   - `KAVSHELL LICENSE /DEL`
   - `KAVSHELL PASSWORD`
   - `KAVSHELL PREVENTION /DISABLE`
   - `KAVSHELL QUARANTINE /ADD`
   - `KAVSHELL QUARANTINE /DELETE`
   - `KAVSHELL REMOTEACCESS`
   - `KAVSHELL RESETMDRMACHINEID`
   - `KAVSHELL SERVERBINDINGDISABLE`
   - `KAVSHELL SIGMA /DISABLE`
   - `KAVSHELL SIGMA /ADD`
   - `KAVSHELL SIGMA /REMOVE>`
   - `KAVSHELL STOP`
   - `KAVSHELL TASK /STOP`
   - `KAVSHELL TELEMETRYFILTERS /IMPORT`

   Caso esta funcionalidade esteja desativada e o usuário atual tenha os direitos necessários, o Kaspersky Embedded Systems Security não solicitará as credenciais. Esta opção é selecionada por padrão.

Caso uma senha vazia do Windows seja definida para o usuário atual, será preciso inserir as credenciais de um usuário que possua os direitos necessários e tenha uma senha não vazia.

7. Insira a senha da conta de usuário KLAdmin.
8. Se necessário, adicione as contas de usuário às quais deseja conceder acesso ao gerenciamento de aplicativos:
   a. Clique **Adicionar**.
      Isso abre o formulário para configurar as permissões de acesso do usuário.
   b. Na janela exibida, selecione o método de adição de usuários: **Adicionar um usuário/grupo de usuários o manualmente**.
   c. Defina um nome de usuário e senha.
   d. Na lista **Permissões**, configure as permissões de acesso do usuário à funcionalidade do aplicativo.
9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como proteger com senha o acesso à funcionalidade do Kaspersky Embedded Systems Security no Console do aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e selecione **Permissões de acesso do usuário para gerenciamento do aplicativo** por meio do menu de contexto do nó.
2. Na janela que é aberta, marque a caixa de seleção **Permitir confirmação de ações com o aplicativo usando credenciais de usuários criadas manualmente**.
3. Caso seja necessário, desmarque a caixa de seleção **Solicitar senha para confirmar ações críticas**.
   Caso esta funcionalidade esteja ativada, o aplicativo solicitará um nome de usuário e senha ao excluir, modificar ou recuperar o aplicativo e ao executar **ações na linha de comando que possam diminuir o nível de proteção do dispositivo.**

   O aplicativo solicita credenciais ao executar os seguintes comandos:

   - `KAVSHELL APPCONTROL`
   - `KAVSHELL APPCONTROL /CONFIG`
   - `KAVSHELL APPCONTROL /GENERATE /import`
   - `KAVSHELL DEVCONTROL`
   - `KAVSHELL EXITPOLICY`
   - `KAVSHELL IMPORT`
   - `KAVSHELL ISOLATION /DISABLE`

- KAVSHELL LICENSE /DEL
- KAVSHELL PASSWORD
- KAVSHELL PREVENTION /DISABLE
- KAVSHELL QUARANTINE /ADD
- KAVSHELL QUARANTINE /DELETE
- KAVSHELL REMOTEACCESS
- KAVSHELL RESETMDRMACHINEID
- KAVSHELL SERVERBINDINGDISABLE
- KAVSHELL SIGMA /DISABLE
- KAVSHELL SIGMA /ADD
- KAVSHELL SIGMA /REMOVE>
- KAVSHELL STOP
- KAVSHELL TASK /STOP
- KAVSHELL TELEMETRYFILTERS /IMPORT

Caso esta funcionalidade esteja desativada e o usuário atual tenha os direitos necessários, o Kaspersky Embedded Systems Security não solicitará as credenciais. Esta opção é selecionada por padrão.

Caso uma senha vazia do Windows seja definida para o usuário atual, será preciso inserir as credenciais de um usuário que possua os direitos necessários e tenha uma senha não vazia.

4. Insira a senha da conta de usuário KLAdmin.
5. Se necessário, adicione as contas de usuário às quais deseja conceder acesso ao gerenciamento de aplicativos:
   a. Clique **Adicionar**.
      Isso abre o formulário para configurar as permissões de acesso do usuário.
   b. Na janela exibida, selecione o método de adição de usuários: **Adicionar um usuário/grupo de usuários o manualmente**.
   c. Defina um nome de usuário e senha.
   d. Na lista **Permissões**, configure as permissões de acesso do usuário à funcionalidade do aplicativo.
6. Salvar alterações.

Como proteger com senha o acesso à funcionalidade do Kaspersky Embedded Systems Security no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Suplementar** → **Permissões de acesso do usuário para gerenciamento do aplicativo** e clique no botão **Configurar**.
5. Na janela que é aberta, marque a caixa de seleção **Permitir confirmação de ações com o aplicativo usando credenciais de usuários criadas manualmente**.
6. Caso seja necessário, desmarque a caixa de seleção **Solicitar senha para confirmar ações críticas**.

   Caso esta funcionalidade esteja ativada, o aplicativo solicitará um nome de usuário e senha ao excluir, modificar ou recuperar o aplicativo e ao executar **ações na linha de comando que possam diminuir o nível de proteção do dispositivo.**

   O aplicativo solicita credenciais ao executar os seguintes comandos:

   - `KAVSHELL APPCONTROL`
   - `KAVSHELL APPCONTROL /CONFIG`
   - `KAVSHELL APPCONTROL /GENERATE /import`
   - `KAVSHELL DEVCONTROL`
   - `KAVSHELL EXITPOLICY`
   - `KAVSHELL IMPORT`
   - `KAVSHELL ISOLATION /DISABLE`
   - `KAVSHELL LICENSE /DEL`
   - `KAVSHELL PASSWORD`
   - `KAVSHELL PREVENTION /DISABLE`
   - `KAVSHELL QUARANTINE /ADD`
   - `KAVSHELL QUARANTINE /DELETE`
   - `KAVSHELL REMOTEACCESS`
   - `KAVSHELL RESETMDRMACHINEID`
   - `KAVSHELL SERVERBINDINGDISABLE`

- KAVSHELL SIGMA /DISABLE
- KAVSHELL SIGMA /ADD
- KAVSHELL SIGMA /REMOVE>
- KAVSHELL STOP
- KAVSHELL TASK /STOP
- KAVSHELL TELEMETRYFILTERS /IMPORT

Caso esta funcionalidade esteja desativada e o usuário atual tenha os direitos necessários, o Kaspersky Embedded Systems Security não solicitará as credenciais. Esta opção é selecionada por padrão.

Caso uma senha vazia do Windows seja definida para o usuário atual, será preciso inserir as credenciais de um usuário que possua os direitos necessários e tenha uma senha não vazia.

7. Insira a senha da conta de usuário KLAdmin.
8. Se necessário, adicione as contas de usuário às quais deseja conceder acesso ao gerenciamento de aplicativos:
   a. Clique **Adicionar**.
      Isso abre o formulário para configurar as permissões de acesso do usuário.
   b. Na janela exibida, selecione o método de adição de usuários: **Adicionar um usuário/grupo de usuários o manualmente**.
   c. Defina um nome de usuário e senha.
   d. Na lista **Permissões**, configure as permissões de acesso do usuário à funcionalidade do aplicativo.
9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Esta senha não pode ser recuperada. A perda da senha resulta na perda total do controle sobre o aplicativo. Além disso, não será impossível remover o aplicativo do dispositivo protegido.

Você pode redefinir a senha a qualquer momento. Para isso, desmarque a caixa de seleção **Permitir confirmação de ações com o aplicativo usando credenciais de usuários criadas manualmente** 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.

Notificações do Secure Desktop

O Kaspersky Embedded Systems Security é compatível com a funcionalidade Secure Desktop. O objetivo desta funcionalidade é confirmar as ações que podem diminuir potencialmente o nível de segurança do computador. Essa funcionalidade permite que um aplicativo exiba uma caixa de diálogo de confirmação isolada de outros processos. Essa funcionalidade utiliza direitos elevados para proteger a solicitação. Dessa forma, apenas o usuário poderá confirmar a ação e não o malware.

O Kaspersky Embedded Systems Security exibe notificações do Secure Desktop para confirmar as seguintes ações:

- Rastreamento ativado ou desativado
- Configurações do aplicativo exportadas ou importadas
- Proteção pausada
- Aplicativo encerrado
- Chave ativa excluída
- Kaspersky Embedded Systems Security desinstalado
- Controle de Dispositivos desativado
- Proteção de arquivos em tempo real desativada
- Política do Kaspersky Security Center desativada
- Relatórios visualizados
- Arquivos restaurados do Backup
- Configurações do Kaspersky Embedded Systems Security modificadas
- Tarefas do aplicativo gerenciadas de outras formas além da inicialização

Como ativar ou desativar as notificações do Secure Desktop no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de propriedades da política, acesse a seção **Configurações do aplicativo**.
4. No bloco **Segurança e confiabilidade**, clique no botão **Configurações**.
5. Uma janela será aberta; nessa janela, selecione a guia **Segurança**.

6. No bloco **Autodefesa**, marque ou desmarque a caixa de seleção **Ativar as notificações do Secure Desktop** para ativar ou desativar as notificações do Secure Desktop.

   Caso os mecanismos de Autodefesa estejam desativados, a caixa de seleção **Ativar as notificações do Secure Desktop** não estará disponível.

7. Feche o cadeado para aplicar a política aos computadores.

8. Clique no botão **OK** para salvar as alterações.

Como ativar ou desativar as notificações do Secure Desktop no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e no painel de resultados, siga o link **Propriedades do aplicativo**.

2. Uma janela será aberta; nessa janela, selecione a guia **Configurações de segurança**.

3. No bloco **Autodefesa**, marque ou desmarque a caixa de seleção **Ativar as notificações do Secure Desktop** para ativar ou desativar as notificações do Secure Desktop.

   Caso os mecanismos de Autodefesa estejam desativados, a caixa de seleção **Ativar as notificações do Secure Desktop** não estará disponível.

4. Clique no botão **OK** para salvar as alterações.

Como ativar ou desativar as notificações do Secure Desktop no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

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

5. No bloco **Segurança e confiabilidade**, clique no botão **Configurar**.

   A janela **Segurança e confiabilidade** é aberta.

6. No bloco **Autodefesa**, marque ou desmarque a caixa de seleção **Ativar as notificações do Secure Desktop** para ativar ou desativar as notificações do Secure Desktop.

   Caso os mecanismos de Autodefesa estejam desativados, a caixa de seleção **Ativar as notificações do Secure Desktop** não estará disponível.

7. Feche o cadeado para aplicar a política aos computadores.

8. Clique no botão **OK** para salvar as alterações.

Zona confiável

Uma *zona confiável* é uma lista de objetos e aplicativos configuradas pelo administrador de sistema que o Kaspersky Embedded Systems Security não monitora quando ativado.

O administrador cria a zona confiável individualmente, considerando as características dos objetos processados e dos aplicativos que estão instalados no computador. Talvez seja necessário incluir objetos e aplicativos na zona confiável se o Kaspersky Embedded Systems Security bloquear o acesso a um objeto ou aplicativo determinado, quando você tem certeza de que ele é inofensivo. Um administrador também pode permitir que um usuário crie sua própria zona confiável local para um computador específico. Dessa forma, os usuários podem criar suas próprias listas locais de exclusões e aplicativos confiáveis, além da zona confiável geral em uma política.

Também é possível adicionar a telemetria EDR para a zona confiável. Isso permite otimizar os dados que o aplicativo envia ao servidor de telemetria para a solução Kaspersky Anti Targeted Attack Platform (EDR).

As exclusões de verificação e os aplicativos confiáveis predefinidos são adicionados à zona confiável. As exclusões de verificação e os aplicativos confiáveis predefinidos ajudam a configurar rapidamente o Kaspersky Embedded Systems sem precisar criar manualmente uma zona confiável.

Criar uma exclusão de verificação

Uma *exclusão de verificação* é um conjunto de condições que devem ser atendidas para que o Kaspersky Embedded Systems Security não verifique um determinado objeto em busca de vírus e outras ameaças.

As exclusões de verificação podem ser usadas pelos seguintes componentes e tarefas do aplicativo:

- **Proteção de Arquivos em Tempo Real**
- **Verificação por demanda**
- **Detecção de Comportamento**
- **Proteção AMSI**
- **Proteção Contra Ameaças à Rede**

O Kaspersky Embedded Systems Security não verifica um objeto se a unidade ou a pasta que contém este objeto estiver incluída no escopo da verificação no início de uma das tarefas de verificação. Contudo, a exclusão de verificação não é aplicada na execução da tarefa de Verificação Personalizada deste objeto.

O Kaspersky Embedded Systems Security não é compatível com as listas de exclusão que contenham mais de cinco mil objetos.

Como criar uma exclusão de verificação no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Suplementar** → **Zona confiável** e clique em **Configurações**.
4. Selecione a guia **Exclusões de verificação**.
5. Marque a caixa de seleção **Mesclar valores ao herdar** se desejar criar uma lista consolidada de exclusões para todos os computadores da empresa. As listas de exclusões nas políticas pai e filho serão mescladas. As listas serão mescladas, desde que a mesclagem de valores ao herdar esteja ativada. Exclusões da política pai são exibidas nas políticas filho em uma exibição somente leitura. Não é possível alterar ou remover exclusões da política pai.
6. Marque a caixa de seleção **Permitir o uso de exclusões locais** se desejar permitir que o usuário crie uma lista local de exclusões. Dessa forma, um usuário pode criar sua própria lista local de exclusões, além da lista geral de exclusões gerada na política. Um administrador pode usar o Kaspersky Security Center para exibir, adicionar, editar ou excluir itens da lista nas propriedades do computador.

   Se a caixa de seleção estiver desmarcada, o usuário poderá acessar apenas a lista geral de exclusões gerada na política. Além disso, caso a caixa de seleção esteja desmarcada, o Kaspersky Embedded Systems Security ocultará a lista consolidada de exclusões de verificação na interface do usuário do aplicativo.
7. Clique em **Adicionar** e selecione uma ação:
   - **Categoria**. É possível agrupar as exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o seu nome e adicione pelo menos uma exclusão de verificação para ela.
   - **Nova exclusão**. O Kaspersky Embedded Systems Security adiciona uma nova exclusão de verificação à raiz da lista.
   - **Nova exclusão para a categoria selecionada**. Para adicionar uma nova exclusão de verificação a uma categoria específica, selecione uma categoria.
   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Embedded Systems Security, é possível adicionar exclusões da lista de exclusões de verificação predefinidas.
8. Para excluir um arquivo ou pasta da verificação, marque a caixa **Arquivo ou pasta**insira o caminho manualmente. Clique no link **Selecionar arquivo ou pasta** para abrir uma janela, e nessa janela, selecione um arquivo ou pasta clicando em **Procurar**.

Também é possível inserir o caminho manualmente. O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:

- O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas.

- Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

- O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.

  É possível usar máscaras no início, no meio ou no final do caminho do arquivo. Por exemplo, caso queira adicionar uma pasta para todos os usuários nas exclusões, insira a máscara `?:\Users\*\Folder\`.

9. Para excluir uma área predefinida da verificação, marque a caixa de seleção **Escopo predefinido**. Clique no link **selecionar escopo predefinido** para abrir uma janela, e nessa janela, selecione um dos escopos padrão no dispositivo protegido.

10. Para excluir os objetos específicos da verificação, marque a caixa de seleção **Tipo do objeto detectado**. Clique no link **inserir nomes do objeto**, clique no botão **Adicionar**, e na janela exibida, insira o nome do tipo de objeto de acordo com a classificação da Kaspersky Encyclopedia (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

    Você pode usar máscaras com o caractere `?` (substitui qualquer caractere único) e o caractere `*` (substitui qualquer número de caracteres). Por exemplo, se a máscara do `Client*` for especificada, o Kaspersky Embedded Systems Security exclui os objetos `Client-IRC`, `Client-P2P` e `Client-SMTP` das verificações.

11. Para excluir um arquivo individual da verificação, marque a caixa de seleção **Hash do objeto**. Clique no link **inserir hash do objeto** para abrir uma janela, e nessa janela, insira um hash do arquivo.

    Se o arquivo for modificado, o hash do arquivo também será modificado. Se isso acontecer, o arquivo modificado não será adicionado às exclusões.

12. Na seção **Escopo de uso da regra**, selecione os componentes aos quais deseja que a exclusão de verificação se aplique.

13. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

14. Salve as alterações para adicionar a exclusão na lista. É possível desativar a exclusão a qualquer momento usando a caixa de seleção ao lado do objeto.

Como criar uma exclusão de verificação no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Suplementar** → **Zona confiável** e clique no botão **Configurar**.
5. Selecione a guia **Exclusões de verificação**.
6. Marque a caixa de seleção **Mesclar valores ao herdar** se desejar criar uma lista consolidada de exclusões para todos os computadores da empresa. As listas de exclusões nas políticas pai e filho serão mescladas. As listas serão mescladas, desde que a mesclagem de valores ao herdar esteja ativada. Exclusões da política pai são exibidas nas políticas filho em uma exibição somente leitura. Não é possível alterar ou remover exclusões da política pai.
7. Marque a caixa de seleção **Permitir o uso de exclusões locais** se desejar permitir que o usuário crie uma lista local de exclusões. Dessa forma, um usuário pode criar sua própria lista local de exclusões, além da lista geral de exclusões gerada na política. Um administrador pode usar o Kaspersky Security Center para exibir, adicionar, editar ou excluir itens da lista nas propriedades do computador.

   Se a caixa de seleção estiver desmarcada, o usuário poderá acessar apenas a lista geral de exclusões gerada na política. Além disso, caso a caixa de seleção esteja desmarcada, o Kaspersky Embedded Systems Security ocultará a lista consolidada de exclusões de verificação na interface do usuário do aplicativo.
8. Clique em **Adicionar** e selecione uma ação:

   - **Categoria**. É possível agrupar as exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o seu nome e adicione pelo menos uma exclusão de verificação para ela.
   - **Nova exclusão**. O Kaspersky Embedded Systems Security adiciona uma nova exclusão de verificação à raiz da lista.
   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Embedded Systems Security, é possível adicionar exclusões da lista de exclusões de verificação predefinidas.
9. Caso queira excluir um arquivo ou pasta da verificação, selecione **Arquivo ou pasta** e marque a caixa de seleção no campo com o mesmo nome. Insira o caminho para o Arquivo ou pasta.

O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:

- O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas.

- Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

- O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.

  É possível usar máscaras no início, no meio ou no final do caminho do arquivo. Por exemplo, caso queira adicionar uma pasta para todos os usuários nas exclusões, insira a máscara `?:\Users\*\Folder\`.

10. Para excluir um escopo predefinido da verificação, selecione **Escopo predefinido**. Na lista suspensa, selecione um dos escopos padrão no dispositivo protegido.

11. Caso queira excluir determinados objetos da verificação, marque a caixa de seleção **Tipo do objeto detectado** e insira o nome do tipo de objeto de acordo com a classificação da Kaspersky Encyclopedia (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

    Você pode usar máscaras com o caractere `?` (substitui qualquer caractere único) e o caractere `*` (substitui qualquer número de caracteres). Por exemplo, se a máscara do `Client*` for especificada, o Kaspersky Embedded Systems Security exclui os objetos *Cliente-IRC*, *Cliente-P2P* e *Cliente-SMTP* das verificações.

12. Para excluir um arquivo individual da verificação, marque a caixa de seleção **Hash do objeto** e adicione um hash de um arquivo ou uma lista de eventos.

    Se o arquivo for modificado, o hash do arquivo também será modificado. Se isso acontecer, o arquivo modificado não será adicionado às exclusões.

13. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

14. Na seção **Componentes de proteção**, selecione os componentes aos quais deseja que a exclusão de verificação se aplique.

15. A nova exclusão será adicionada à lista. É possível desativar a exclusão a qualquer momento usando a caixa de seleção na coluna **Status**.

16. Salvar alterações.

Como criar uma exclusão de verificação no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e selecione **Zona confiável** por meio do menu de contexto do nó.

   A janela **Configurar a Zona confiável** é aberta.

2. Na seção **Exclusões**, clique no botão **Configurações** ao lado do bloco **Exclusões de verificação**.

3. Clique em **Adicionar** e selecione uma ação:

   - **Categoria**. É possível agrupar as exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o seu nome e adicione pelo menos uma exclusão de verificação para ela.
   - **Nova exclusão**. O Kaspersky Embedded Systems Security adiciona uma nova exclusão de verificação à raiz da lista.
   - **Nova exclusão para a categoria selecionada**. Para adicionar uma nova exclusão de verificação a uma categoria específica, selecione uma categoria.
   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Embedded Systems Security, é possível adicionar exclusões da lista de exclusões de verificação predefinidas.

4. Para excluir um arquivo ou pasta da verificação, marque a caixa **Arquivo ou pasta**insira o caminho manualmente. Clique no link **Selecionar arquivo ou pasta** para abrir uma janela, e nessa janela, selecione um arquivo ou pasta com um clique em **Procurar**.

   Também é possível inserir o caminho manualmente. O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:

   - O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas.
   - Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.
   - O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/`(delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.

     É possível usar máscaras no início, no meio ou no final do caminho do arquivo. Por exemplo, caso queira adicionar uma pasta para todos os usuários nas exclusões, insira a máscara `?:\Users\*\Folder\`.

5. Para excluir uma área predefinida da verificação, marque a caixa de seleção **Escopo predefinido**. Clique no link **selecionar escopo predefinido** para abrir uma janela, e nessa janela, selecione um dos escopos padrão no dispositivo protegido.

6. Para excluir os objetos específicos da verificação, marque a caixa de seleção **Tipo do objeto detectado**. Clique no link **inserir nomes do objeto**, clique no botão **Adicionar**, e na janela exibida, insira o nome do tipo de objeto de acordo com a classificação da Kaspersky Encyclopedia (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

   Você pode usar máscaras com o caractere `?` (substitui qualquer caractere único) e o caractere `*` (substitui qualquer número de caracteres). Por exemplo, se a máscara do `Client*` for especificada, o Kaspersky Embedded Systems Security exclui os objetos `Client-IRC`, `Client-P2P` e `Client-SMTP` das verificações.

7. Para excluir um arquivo individual da verificação, marque a caixa de seleção **Hash do objeto**. Clique no link **inserir hash do objeto** para abrir uma janela, e nessa janela, insira um hash do arquivo.

   Se o arquivo for modificado, o hash do arquivo também será modificado. Se isso acontecer, o arquivo modificado não será adicionado às exclusões.

8. Na seção **Escopo de uso da regra**, selecione os componentes aos quais deseja que a exclusão de verificação se aplique.

9. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

10. Salve as alterações para adicionar a exclusão na lista. É possível desativar a exclusão a qualquer momento usando a caixa de seleção ao lado do objeto.

Exemplos de máscara de caminho:
Caminhos a arquivos localizaram em qualquer pasta:

- A máscara `*.exe` incluirá todos os caminhos para os arquivos que têm a extensão exe.
- A máscara `example*` incluirá todos os caminhos para os arquivos nomeados EXAMPLE.

Caminhos a arquivos localizaram em uma pasta especificada:

- A máscara `C:\dir\*.*` incluirá todos os caminhos para arquivos localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
- A máscara `C:\dir\*` incluirá todos os caminhos para os arquivos localizados na pasta C:\dir\, inclusive as subpastas.
- A máscara `C:\dir\` incluirá todos os caminhos para os arquivos localizados na pasta C:\dir\, inclusive as subpastas.
- A máscara `C:\dir\*.exe` incluirá todos os caminhos para arquivos com a extensão EXE localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
- A máscara `C:\dir\test` incluirá todos os caminhos para arquivos nomeados "teste" localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
- A máscara `C:\dir\*\test` incluirá todos os caminhos para arquivos nomeados "teste" localizados na pasta C:\dir\ e nas subpastas de C:\dir\.
- A máscara `C:\dir1\*\dir3\` incluirá todos os caminhos para arquivos nas subpastas dir3 um nível abaixo da pasta C:\dir1\.
- A máscara `C:\dir1\**\dirN\` incluirá todos os caminhos para arquivos nas subpastas dirN na pasta C:\dir1\ em qualquer nível.

Caminhos para arquivos localizados em todas as pastas com um nome especificado:

- A máscara `dir\*.*` incluirá todos os caminhos para arquivos nas pastas denominadas “dir”, mas não nas subpastas dessas pastas.
- A máscara `dir\*` incluirá todos os caminhos para arquivos nas pastas denominadas “dir”, mas não nas subpastas dessas pastas.
- A máscara `dir\` incluirá todos os caminhos para arquivos nas pastas denominadas “dir”, mas não nas subpastas dessas pastas.
- A máscara `dir\*.exe` incluirá todos os caminhos para arquivos com a extensão EXE em pastas nomeadas “dir”, mas não nas subpastas dessas pastas.
- A máscara `dir\test` incluirá todos os caminhos para arquivos nomeados "teste" em pastas nomeadas “dir”, mas não nas subpastas dessas pastas.

Selecionar tipos de objetos detectáveis

Para selecionar os tipos objetos detectáveis:

1. Na árvore do Console do Aplicativo, selecione o node **Kaspersky Embedded Systems Security** e execute uma das seguintes ações:
   - Clique no link **Configurar a Zona confiável** no painel de resultados do node.
   - Selecione **Zona confiável** no menu de contexto do node.

   A janela **Configurar a Zona confiável** é aberta.
2. Na seção **Tipos de objetos detectados**, clique no botão **Configurações**.

3. Na janela exibida, marque as caixas de seleção em frente aos tipos de objetos que deseja detectar com o Kaspersky Embedded Systems Security:

   - **Vírus e worms**.

     Subcategoria: vírus e worms (Vírus_e_Worms)

     Nível de perigo: alto

     Os vírus e worms clássicos executam ações que não são autorizadas pelo usuário. Eles podem criar cópias de si mesmos capazes de se autoduplicar.

     Vírus clássico

     Quando um vírus clássico infiltra um computador, ele infecta um arquivo, ativa, executa ações maliciosas e adiciona cópias de si mesmo em outros arquivos.

     Um vírus clássico multiplica-se apenas em recursos locais do computador; ele não pode penetrar em outros computadores sozinho. Ele pode ser passado a outro computador apenas se adicionar uma cópia de si mesmo a um arquivo armazenado em uma pasta compartilhada ou em um CD inserido, ou se o usuário encaminhar uma mensagem de e-mail com um arquivo infectado anexado.

     O código do vírus clássico pode penetrar várias áreas de computadores, sistemas operacionais e aplicativos. Dependendo do ambiente, os vírus são divididos em *vírus de arquivo*, *vírus de reinicialização*, *vírus de script* e *vírus de macro*.

     Os vírus podem infectar arquivos usando várias técnicas. Os vírus de *sobreposição* gravam o seu código sobre o código do arquivo que é infectado, apagando assim o conteúdo do arquivo. O arquivo infectado deixa de funcionar e não pode ser restaurado. Os vírus *parasíticos* modificam arquivos, deixando-os totalmente ou parcialmente funcionais. Os *vírus companheiros* não modificam arquivos, mas em vez disso criam réplicas. Quando um arquivo infectado é aberto, uma réplica dele (o que é de fato um vírus) é iniciada. Os seguintes tipos de vírus também são encontrados: *vírus de link*, *Vírus OBJ*, *Vírus LIB*, vírus de *código-fonte* e muitos outros.

     Worm

     Como com um vírus clássico, o código de um worm é ativado e executa ações maliciosas depois que se infiltrar em um computador. Os worms são assim denominados por causa da sua capacidade de "rastejar" de um computador para outro e disseminar cópias via canais de dados numerosos sem a permissão do usuário.

     O recurso principal que permite diferenciar entre vários tipos de worms é o modo como eles se disseminam. A seguinte tabela fornece um resumo de vários tipos de worms, que são classificados pelo modo como eles se disseminam.

Os caminhos pelos quais os worms se disseminam

Tipo	Name	Descrição
Worm de e-mail	Worm de e-mail	Eles se espalham através do e-mail. Uma mensagem de e-mail infectada contém um arquivo anexado com uma cópia de um worm ou link para um arquivo de que é carregado a um site que pode ter sido invadido ou criado exclusivamente com esse objetivo. Quando você abre o arquivo anexo, o worm é ativado. Quando você clica no link, baixa e depois abre o arquivo, o worm também inicia a execução das suas ações maliciosas. Depois disso, ele continua disseminando cópias de si mesmo, procurando outros endereços de e-mail e enviando mensagens infectadas.
IM-Worm	Worms de cliente de MI	Eles se disseminam através de clientes de MI. Normalmente, esses worms enviam mensagens que contêm um link para um arquivo com uma cópia do worm em um site, utilizando as listas de contato do usuário. Quando o usuário baixa e abre o arquivo, o worm é ativado.
IRC-Worm	Worms de bate-papo da Internet	Eles se disseminam através de Bate-papos relé da Internet, sistemas de serviço que permitem se comunicar com outras pessoas pela Internet em tempo real. Esses worms publicam um arquivo com uma cópia de si mesmos ou um link para o arquivo em um bate-papo da Internet. Quando o usuário baixa e abre o arquivo, o worm é ativado.
Worm de rede	Worms de rede	Estes worms se disseminam por redes de computador. Diferentemente de outros tipos de worms, um worm de rede típico dissemina-se sem a participação do usuário. Ele verifica a rede local quanto a computadores que contêm programas com vulnerabilidades. Para fazer isso, ele envia um pacote de rede especialmente formado (exploit) que contém o código do worm ou uma parte dele. Se um computador "vulnerável" estiver na rede, ele receberá esse pacote de rede. Quando o worm penetra completamente o computador, ele é ativado.
Worm de P2P	Worms de rede de compartilhamento de arquivo	Eles se disseminam por redes de compartilhamento de arquivo ponto a ponto. Para infiltrar uma rede P2P, o worm faz uma cópia de si mesmo em uma pasta de compartilhamento de arquivo normalmente localizada no computador do usuário. A rede P2P exibe informações sobre esse arquivo para que o usuário possa "encontrar" o arquivo infectado na rede como qualquer outro arquivo, e então baixá-lo e abri-lo. Os worms mais sofisticados emulam o protocolo de rede de uma rede P2P específica: eles devolvem respostas positivas a perguntas de pesquisa e oferecem cópias de si mesmos para download.
Worm	Outros tipos de worms	Outros tipos de worms incluem: • Worms que disseminam cópias de si mesmos em recursos de rede. Usando as funções do sistema operacional, eles verificam pastas de rede disponíveis, conectam-se a computadores na Internet e tentam obter acesso total às suas unidades de disco. Diferentemente dos tipos de worms anteriormente descritos, outros tipos de worms não são ativados sozinhos, mas quando o usuário abre um arquivo que contém uma cópia do worm. • Os worms que não usam nenhum dos métodos descritos na tabela anterior para se propagar (por exemplo, aqueles que se propagam pelos telefones celulares).

- **Cavalos de Troia**.

  Subcategoria: Cavalos de Troia

  Nível de perigo: alto

  Diferentemente de worms e vírus, os Cavalos de Troia não se autoduplicam. Por exemplo, eles penetram um computador através do e-mail ou de um navegador quando o usuário visita uma página da Web infectada. Os Cavalos de Troia são iniciados com a participação do usuário. Eles começam a executar as suas ações maliciosas logo depois que eles são iniciados.

  Os Cavalos de Troia comportam-se de maneira diferente em computadores infectados. As funções principais de Cavalos de Troia consistem em bloquear, modificar ou destruir informações e incapacitar computadores ou redes. Os Cavalos de Troia também podem receber ou enviar arquivos, executá-los, exibir mensagens na tela, solicitar páginas da Web, baixar e instalar programas, além de reiniciar o computador.

Os hackers muitas vezes usam "conjuntos" de vários Cavalos de Troia.

Os tipos de comportamento de Cavalo de Troia são descritos na seguinte tabela.

Tipos de comportamento de Cavalo de Troia em um computador infectado

Tipo	Name	Descrição
Trojan-ArcBomb	Cavalos de Troia – "bombas de arquivos compactados"	Quando descompactados, estes arquivos compactados crescem a tal ponto que a operação do computador é afetada. Quando o usuário tenta descompactar esse arquivo compactado, o computador pode ficar lento ou travar; o disco rígido pode ficar cheio de dados "vazios". "As bombas de arquivo compactado" são especialmente perigosas para arquivo e servidores de e-mail. Se o servidor usar um sistema automático para processar informações recebidas, uma "bomba de arquivo compactado" poderá parar o servidor.
Backdoor	Cavalos de Troia para administração remota	Eles são considerados os tipos mais perigosos de Cavalo de Troia. Nas suas funções, eles são semelhantes a aplicativos de administração remota que são instalados em computadores. Estes programas instalam-se no computador sem ser notados pelo usuário, permitindo ao intruso gerenciar o computador remotamente.
Cavalo de Troia	Cavalos de Troia	Eles incluem os seguintes aplicativos maliciosos: • **Cavalos de Troia clássicos**. Estes programas executam apenas as funções principais de Cavalos de Troia: bloqueio, modificação ou destruição de informações e incapacitação de computadores ou redes. Eles não têm recursos avançados, diferentemente de outros tipos de Cavalos de Troia que são descritos na tabela. • **Cavalos de Troia versáteis**. Estes programas têm recursos avançados típicos de vários tipos de Cavalos de Troia.
Trojan-Ransom	Cavalos de Troia de resgate	Eles tomam as informações do usuário como "refém", modificando-as ou bloqueando-as, ou afetam a operação do computador para que o usuário perca a capacidade de usar informações. O intruso exige um resgate do usuário, prometendo enviar um aplicativo para restaurar o desempenho do computador e os dados que estavam armazenados nele.
Trojan-Clicker	Clicadores de Cavalo de Troia	Eles acessam páginas da Web do computador do usuário, enviando comandos a um navegador por conta própria ou modificando os endereços da Web especificados em arquivos do sistema operacional. Usando esses programas, os intrusos cometem ataques de rede e aumentam as visitas de site, aumentando o número de exibições de anúncios de banner.
Trojan-Downloader	Downloaders de Cavalo de Troia	Eles acessam a página da Web do intruso, baixam dela outros aplicativos maliciosos e os instalam no computador do usuário. Eles podem conter o nome do arquivo do aplicativo malicioso para baixar ou recebê-lo da página da Web que é acessada.
Trojan-Dropper	Droppers de Cavalo de Troia	Eles contêm outros Cavalos de Troia que eles instalam no disco rígido e depois se instalam. Os intrusos podem usar programas do tipo dropper de Cavalo de Troia com os seguintes objetivos: • Instalar um aplicativo malicioso sem ser notado pelo usuário: aplicativos do tipo Dropper de Cavalo de Troia não exibem nenhuma mensagem ou exibem mensagens falsas que informam, por exemplo, sobre um erro em um arquivo compactado ou uma versão incompatível do sistema operacional. • Proteja outro aplicativo malicioso conhecido contra detecção: nem todos os softwares de antivírus pode detectar um programa malicioso dentro de um programa do tipo instalador de Cavalos de Tróia.
Trojan-Notifier	Notificadores de Cavalo de Troia	Eles informam a um intruso que o computador infectado está acessível, enviando-o informações sobre o computador: Endereço IP, número da porta aberta ou endereço de e-mail. Eles se conectam ao intruso via e-mail, FTP, acessando a página da Web do intruso ou de outro modo. Os programas do tipo notificador de Cavalo de Troia muitas vezes são usados em conjuntos que são feitos de vários Cavalos de Troia. Eles notificam o intruso que outros Cavalos de Troia foram instalados com sucesso no computador do usuário.
Trojan-Proxy	Proxies de Cavalo de Troia	Eles permitem ao intruso acessar anonimamente páginas da Web usando o computador do usuário; eles muitas vezes são usados para enviar spam.

Tipo	Name	Descrição
Trojan-PSW	Password-stealing-ware	O password-stealing-ware é uma espécie de Cavalo de Troia que rouba contas de usuário, como dados de registro de software. Esses Cavalos de Troia encontram dados confidenciais em arquivos do sistema e no registro e os enviam ao "invasor" por e-mail, via FTP, acessando a página da web do intruso ou de outro modo. Alguns desses Cavalos de Troia são categorizados por tipos separados que são descritos nesta tabela. Estes são Cavalos de Troia que roubam contas bancárias (Trojan-Banker), roubam dados de usuários de clientes de MI (Trojan-IM) e roubam informações de usuários de jogos on-line (Trojan-GameThief).
Trojan-Spy	Espiões de Cavalo de Troia	Eles espiam o usuário, coletando informações sobre as ações que o usuário faz ao trabalhar no computador. Eles podem interceptar os dados que o usuário insere no teclado, fazer capturas de tela ou coletar listas de aplicativos ativos. Depois de receber as informações, eles as transferem para o intruso por e-mail, via FTP, acessando a página da Web do intruso ou de outro modo.
Trojan-DDoS	Atacantes de rede de Cavalo de Troia	Eles enviam inúmeras solicitações do computador do usuário a um servidor remoto. O servidor não tem recursos para processar todas as solicitações, portanto deixa de funcionar (Negação de Serviço, ou simplesmente DoS). Os hackers muitas vezes infectam muitos computadores com esses programas para que eles possam usar os computadores para atacar um único servidor simultaneamente. Os programas de DoS cometem um ataque de um único computador com o conhecimento do usuário. Os programas DDoS (DoS Distribuído) cometem ataques distribuídos de vários computadores sem ser notados pelo usuário do computador infectado.
Trojan-IM	Cavalos de Troia que roubam informações de usuários de clientes de MI	Eles roubam números de contas e senhas de usuários de MI cliente. Eles transferem os dados para o intruso por e-mail, via FTP, acessando a página da Web do intruso ou de outro modo.
Rootkit	Rootkits	Eles mascaram outros aplicativos maliciosos e a sua atividade, prolongando assim a persistência dos aplicativos no sistema operacional. Eles também podem esconder arquivos, processos na memória de um computador infectado ou chaves de registro que executam aplicativos maliciosos. Os rootkits podem mascarar a troca de dados entre aplicativos no computador do usuário e em outros computadores na rede.
Trojan-SMS	Cavalos de Troia na forma de mensagens de SMS	Eles infectam telefones celulares, enviando mensagens de SMS a números de telefone de tarifa premium.
Trojan-GameThief	Cavalos de Troia que roubam informações de usuários de jogos on-line	Eles roubam as credenciais da conta de usuários de jogos on-line; após o qual eles enviam os dados ao invasor por e-mail, através de FTP, ao acessar a página da web do invasor ou de outro modo.
Trojan-Banker	Cavalos de Troia que roubam contas bancárias	Eles roubam dados de conta bancária ou dados do sistema de moeda eletrônica, enviam os dados ao hacker por e-mail, através de FTP, ao acessar a página da web do hacker ou outro meio.
Trojan-Mailfinder	Cavalos de Troia que coletam endereços de e-mail	Eles coletam endereços de e-mail armazenados em um computador e os enviam ao intruso por e-mail, via FTP, acessando a página da Web do intruso ou de outro modo. Os intrusos podem enviar spam aos endereços que eles coletaram.

- **Ferramentas maliciosas**.

  Subcategoria: Ferramentas maliciosas

  Nível de perigo: médio

  Diferentemente de outros tipos de malware, as ferramentas maliciosas não executam as suas ações logo depois que elas são iniciadas. Elas podem ser armazenadas com segurança e iniciadas no computador do usuário. Os intrusos muitas vezes usam os recursos destes programas para criar vírus, worms e Cavalos de Troia, cometer ataques de rede em servidores remotos, computadores de hack ou executar outras ações maliciosas.

  Vários recursos de ferramentas maliciosas são agrupados pelos tipos descritos na seguinte tabela.

Recursos de ferramentas maliciosas

Tipo	Name	Descrição
Construtor	Construtores	Eles permitem criar novos vírus, worms e Cavalos de Troia. Alguns construtores contam com uma interface baseada em janelas padrão na qual o usuário pode selecionar o tipo de aplicativo malicioso a ser criado, o modo de anular aplicativos de depuração e outros recursos.
DoS	Ataques de rede	Eles enviam inúmeras solicitações do computador do usuário a um servidor remoto. O servidor não tem recursos para processar todas as solicitações, portanto deixa de funcionar (Negação de Serviço, ou simplesmente DoS).
Exploit	Exploits	Um *exploit* é um grupo de dados ou um código de programa que usa vulnerabilidades do aplicativo no qual é processado, executando uma ação maliciosa no computador. Por exemplo, um exploit pode gravar ou ler arquivos ou solicitar páginas da Web "infectadas". Exploits diferentes usam vulnerabilidades em aplicativos ou serviços de rede diferentes. Disfarçado como um pacote de rede, um exploit é transmitido pela rede para vários computadores, procurando computadores com serviços de rede vulneráveis. Um exploit em um arquivo DOC usa as vulnerabilidades de um editor de texto. Ela pode iniciar a execução das ações que são pré-programadas pelo hacker quando o usuário abre o arquivo infectado. Um exploit incorporado em uma mensagem de e-mail procura vulnerabilidades em qualquer cliente de e-mail. Ela pode iniciar a execução de uma ação maliciosa logo depois que o usuário abre a mensagem infectada neste cliente de e-mail. Os worms de rede disseminam-se pelas redes usando exploits. Nuker exploits são pacotes de rede que desativam os computadores.
FileCryptor	Criptadores	Eles criptografam outros aplicativos maliciosos para escondê-los do aplicativo antivírus.
Flooder	Programas para "contaminar" redes	Eles enviam várias mensagens através de canais de rede. Este tipo de ferramentas inclui, por exemplo, programas que contaminam Bate-papos relé da Internet. As ferramentas do tipo Flooder não incluem programas que "contaminam" canais usados por e-mail, clientes de MI e sistemas de comunicação móvel. Esses programas são diferenciados como tipos separados que são descritos na tabela (E-mail-Flooder, MI-Flooder e SMS-Flooder).
HackTool	Ferramentas de invasão	Elas permitem invadir o computador no qual elas são instaladas ou atacam outro computador (por exemplo, adicionando novas contas de sistema sem a permissão do usuário ou apagando registros do sistema para esconder rastros da sua presença no sistema operacional). Este tipo de ferramentas inclui alguns sniffers que apresentam funções maliciosas, como interceptação de senha. Os sniffers são programas que permitem exibir o tráfego de rede.
Hoax	Hoaxes	Eles alarmam o usuário por mensagens parecidas com um vírus: eles podem "detectar um vírus" em um arquivo não infectado ou notificar o usuário de que o disco foi formatado, embora isto não tenha acontecido na verdade.
Spoofer	Ferramentas de falsificação	Elas enviam mensagens e solicitações de rede com um endereço falso do remetente. Os intrusos usam ferramentas do tipo Spoofer para se fazer passar por remetentes verdadeiros de mensagens, por exemplo.
VirTool	Ferramentas que modificam aplicativos maliciosos	Elas permitem modificar outros programas de malware, escondendo-os de aplicativos antivírus.
Email-Flooder	Programas que "contaminam" endereços de e-mail	Eles enviam inúmeras mensagens a vários endereços de e-mail, "contaminando-os". Um grande volume de mensagens recebidas impede usuários de exibir mensagens úteis nas suas caixas de entrada.
IM-Flooder	Programas que "contaminam" o tráfego de clientes de MI	Eles inundam usuários de clientes de MI com mensagens. Um grande volume de mensagens impede usuários de exibir mensagens recebidas úteis.
SMS-Flooder	Programas que "contaminam" o tráfego com mensagens de SMS	Eles enviam mensagens de SMS numerosas a telefones celulares.

- **Adware**.

  Subcategoria: software publicitário (Adware);

Nível de perigo: médio

O adware exibe a informação publicitária ao usuário. Os programas de adware exibem anúncios de banner nas interfaces de outros programas e redirecionam perguntas de pesquisa para páginas da Web publicitárias. Alguns deles coletam informações de marketing sobre o usuário e as enviam ao desenvolvedor: estas informações podem incluir os nomes dos sites que são visitados pelo usuário ou o conteúdo das perguntas de pesquisa do usuário. Diferentemente de programas do tipo espião de Cavalo de Troia, o adware envia essas informações ao desenvolvedor com a permissão do usuário.

- **Discadores automáticos**.

  Subcategoria: Discadores automáticos (discador).

  Nível de perigo: médio

  Os discadores automáticos podem estabelecer conexões telefônicas discretamente com o uso de um modem.

- **Software legítimo que pode ser usado por intrusos para danificar seu computador ou dados pessoais**.

  Subcategoria: software legal que pode ser usado por criminosos para danificar o seu computador ou dados pessoais.

  Nível de perigo: médio

  A maioria destes aplicativos é úteis, muitos usuários os executam. Esses aplicativos incluem clientes IRC, discadores automáticos, programas de download de arquivo, monitores de atividade do sistema de computação, utilitários de senha e servidores de Internet para FTP, HTTP e Telnet.

  Contudo, se os intrusos ganham o acesso a esses programas, ou se eles os colocam no computador do usuário, alguns recursos do aplicativo podem ser usados para violar a segurança.

  Esses aplicativos diferenciam-se pela função; os seus tipos são descritos na seguinte tabela.

Tipo	Name	Descrição
Client-IRC	Clientes de bate-papo da Internet	Os usuários instalam estes programas para falar com pessoas em Bate-papos relé da Internet. Os intrusos usam os programas para disseminar malware.
Downloader	Programas para download	Eles podem baixar arquivos de páginas da Web no modo oculto.
Monitor	Programas para monitoramento	Eles permitem monitorar a atividade sobre o computador no qual eles são instalados (vendo quais aplicativos estão ativos e como eles trocam dados com aplicativos instalados em outros computadores).
PSWTool	Restauradores de senha	Eles permitem exibir e restaurar senhas esquecidas. Os intrusos implantam-nos em segredo em computadores de usuários com o mesmo objetivo.
RemoteAdmin	Programas de administração remota	Eles são amplamente usados por administradores de sistema. Estes programas permitem obter o acesso à interface de um computador remoto para controlá-lo e gerenciá-lo. Os intrusos implantam-nos em segredo em computadores de usuários com o mesmo objetivo: monitorar e gerenciar computadores remotos. Os programas de administração remota legais diferenciam-se de Cavalos de Troia do tipo Backdoor para administração remota. Os Cavalos de Troia têm a capacidade de penetrar o sistema operacional independentemente e instalar-se; os programas legais são incapazes de fazer isso.
Server-FTP	Servidores FTP	Eles funcionam como servidores FTP. Os intrusos implantam-nos no computador do usuário para abrir o acesso remoto via FTP.

Tipo	Name	Descrição
Server-Proxy	Servidores proxy	Eles funcionam como servidores proxy. Os intrusos implantam-nos no computador do usuário para enviar spam em nome do usuário.
Server-Telnet	Servidores Telnet	Eles funcionam como servidores Telnet. Os intrusos implantam-nos no computador do usuário para abrir o acesso remoto via Telnet.
Server-Web	Servidores Web	Eles funcionam como servidores Web. Os intrusos implantam-nos no computador do usuário para abrir o acesso remoto via HTTP.
RiskTool	Ferramentas para trabalhar em um computador local	Elas fornecem ao usuário opções adicionais trabalhando no próprio computador do usuário. As ferramentas permitem ao usuário ocultar arquivos ou janelas de aplicativos ativos e encerrar processos ativos.
NetTool	Ferramentas de rede	Elas fornecem ao usuário opções adicionais trabalhando com outros computadores na rede. Essas ferramentas permitem reiniciá-los, detectando portas abertas e iniciando aplicativos instalados nos computadores.
Client-P2P	Clientes de rede P2P	Eles permitem trabalhar em redes ponto a ponto. Eles podem ser usados por intrusos para disseminar o malware.
Client-SMTP	Clientes de SMTP	Eles enviam mensagens de e-mail sem o conhecimento do usuário. Os intrusos implantam-nos no computador do usuário para enviar spam em nome do usuário.
WebToolbar	Barras de ferramentas da Web	Elas adicionam barras de ferramentas às interfaces de outros aplicativos para usar motores de busca.
FraudTool	Pseudoprogramas	Eles se fazem passar por outros programas. Por exemplo, há programas de pseudoantivírus que exibem mensagens sobre a detecção de malware. Contudo, na verdade, eles não encontram nem desinfetam nada.

- **Objetos cuja compactação pode ser usada para proteger códigos maliciosos**.

  Subcategoria: Arquivos compactados que podem causar danos.

  Nível de perigo: médio.

  O arquivo é compactado por meio de um compactador especial usado para compactar malware: vírus, worms, cavalos de Troia. O Kaspersky Embedded Systems Security verifica o módulo descompactador dentro de arquivos compactados SFX (autoextraíveis).

  Para ocultar o malware da detecção por um antivírus, os hackers compactam-no com o uso de compactadores especiais. Os especialistas da Kaspersky identificaram os compactadores mais populares entre hackers.

- **Objetos em vários pacotes**.

  Subcategoria: Arquivos com várias compactações.

  Nível de perigo: médio.

  O arquivo é compactado com um ou mais compactadores e por três vezes ou mais.

  Para ocultar o malware da detecção por um antivírus, os hackers podem compactar um arquivo várias vezes. O Kaspersky Embedded Systems Security verifica arquivos compactados.

4. Salvar alterações.

Editar a lista de aplicativos confiáveis

A *lista de aplicativos confiáveis* é uma lista de aplicativos cuja atividade de arquivo e rede (inclusive atividade maliciosa) e acesso ao registro do sistema e que não são monitorados pelo Kaspersky Embedded Systems Security. Por padrão, o Kaspersky Embedded Systems Security monitora todos os objetos que são abertos, executados ou salvos por qualquer processo do aplicativo e controla a atividade de todos os aplicativos e tráfego de rede criada por eles. Depois que um aplicativo é adicionado à lista de aplicativos confiáveis, o Kaspersky Embedded Systems Security para de monitorar a atividade do aplicativo.

A diferença entre exclusões de verificação e aplicativos confiáveis é que, para as exclusões, o Kaspersky Embedded Systems Security não verifica arquivos, enquanto para os aplicativos confiáveis, o componente não controla os processos iniciados. Se um aplicativo confiável criar um arquivo malicioso em uma pasta que não esteja incluída nas exclusões de verificação, o Kaspersky Embedded Systems Security detectará o arquivo e eliminará a ameaça. Se a pasta for adicionada às exclusões, o Kaspersky Embedded Systems Security ignorará este arquivo.

Por exemplo, se os objetos usados pelo Bloco de notas do Microsoft Windows forem considerados seguros, ou seja, se você confia nesse aplicativo, adicione o Bloco de notas do Microsoft Windows à lista de aplicativos confiáveis para que os objetos usados por esse aplicativo não sejam monitorados. Isso aumentará o desempenho do computador, o que é especialmente importante ao usar aplicativos de servidor.

Além disso, algumas ações classificadas como suspeitas pelo Kaspersky Embedded Systems Security podem ser consideradas seguras por vários aplicativos. Por exemplo, a interceptação de dados digitados no teclado é um processo de rotina dos programas que alternam automaticamente o layout do teclado (como o Punto Switcher). Para considerar as especificidades desses aplicativos e desativar o monitoramento de suas atividades, é recomendável adicioná-los à lista de aplicativos confiáveis.

Os aplicativos confiáveis ajudam a evitar problemas de compatibilidade entre o Kaspersky Embedded Systems Security e outros aplicativos (por exemplo, o problema de verificação dupla do tráfego de rede de um computador de terceiros pelo Kaspersky Embedded Systems Security e por outro aplicativo antivírus).

Ao mesmo tempo, o arquivo executável e o processo do aplicativo confiável são verificados para detectar vírus e outro tipo de malware. Um aplicativo pode ser excluído completamente da verificação do Kaspersky Embedded Systems Security por meio das exclusões de verificação.

O Kaspersky Embedded Systems Security não é compatível com as listas de aplicativos confiáveis que contenham mais de cinco mil objetos.

Como adicionar um aplicativo à lista confiável no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Suplementar**.
4. No bloco **Zona confiável**, clique no botão **Configurações**.
5. Na janela que é aberta, selecione a guia **Aplicativos confiáveis**.

   Essa ação abre uma janela que contém uma lista dos aplicativos confiáveis.

6. Marque a caixa de seleção **Não verificar operações de backup de arquivos** caso queira ignorar verificação de operações de leitura de arquivo caso tais operações sejam executadas por ferramentas de backup instaladas no dispositivo protegido.

7. Marque a caixa de seleção **Mesclar valores ao herdar** se deseja criar uma lista consolidada de aplicativos confiáveis para todos os computadores da empresa. As listas de aplicativos confiáveis nas políticas pai e filho serão mescladas. As listas serão mescladas, desde que a mesclagem de valores ao herdar esteja ativada. Aplicativos confiáveis da política pai são exibidos nas políticas filho em uma exibição somente leitura. Não é possível alterar ou excluir aplicativos confiáveis da política pai

8. Marque a caixa de seleção **Permitir a edição de aplicativos locais confiáveis** se deseja permitir que o usuário crie uma lista local de aplicativos confiáveis. Dessa forma, um usuário pode criar sua própria lista local de aplicativos confiáveis, além da lista geral de aplicativos confiáveis gerada na política. Um administrador pode usar o Kaspersky Security Center para exibir, adicionar, editar ou excluir itens da lista nas propriedades do computador.

   Se a caixa de seleção estiver desmarcada, o usuário poderá acessar apenas a lista geral de aplicativos confiáveis gerada na política. Além disso, caso a caixa de seleção esteja desmarcada, o Kaspersky Embedded Systems Security ocultará a lista consolidada de aplicativos confiáveis na interface do usuário do aplicativo.

9. Marque a caixa de seleção **Não verificar a atividade dos arquivos dos processos especificados** para ignorar a verificação das operações do arquivo para processos confiáveis.

10. Clique em **Adicionar** e selecione uma ação:

    - **Categoria**. É possível agrupar aplicativos confiáveis em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione pelo menos um aplicativo confiável para ela.
    - **Nova exclusão**. O Kaspersky Embedded Systems Security adiciona um novo aplicativo confiável à raiz da lista.
    - **Nova exclusão para a categoria selecionada**. Para adicionar um novo aplicativo confiável a uma categoria específica, selecione uma categoria.
    - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Embedded Systems Security, é possível adicionar aplicativos da lista de aplicativos confiáveis predefinidos.

11. Na janela aberta, marque a caixa de seleção **Use o caminho inteiro do processo no disco para saber se é confiável** e insira o caminho para determinar se o processo é confiável.

    O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:

    > O Kaspersky Embedded Systems Security não é compatível com a variável de ambiente `%userprofile%` ao gerar uma lista de aplicativos confiáveis no console do Kaspersky Security Center. Para aplicar a entrada em todas as contas de usuários, é possível utilizar o caractere * (por exemplo, `C:\Users\*\Documents\File.exe`). Quando adicionar uma nova variável de ambiente, é necessário reiniciar o aplicativo.

12. Defina as configurações avançadas para o aplicativo confiável (consulte a tabela abaixo).

13. Clique **OK**.

    O novo aplicativo confiável será adicionado à lista. Você pode excluir um aplicativo da zona confiável a qualquer momento usando a caixa de seleção ao lado do objeto.

14. Salvar alterações.

Como adicionar um aplicativo na lista confiável no Kaspersky Security Center Web Console

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

4. Selecione a guia **Configurações do aplicativo**.
5. Vá para **Suplementar** → **Zona confiável** e clique no botão **Configurar**.
6. Na janela que é aberta, selecione a guia **Aplicativos confiáveis**.
7. Marque a caixa de seleção **Não verificar operações de backup de arquivos** caso queira ignorar verificação de operações de leitura de arquivo caso tais operações sejam executadas por ferramentas de backup instaladas no dispositivo protegido.
8. Marque a caixa de seleção **Mesclar valores ao herdar** se deseja criar uma lista consolidada de aplicativos confiáveis para todos os computadores da empresa. As listas de aplicativos confiáveis nas políticas pai e filho serão mescladas. As listas serão mescladas, desde que a mesclagem de valores ao herdar esteja ativada. Aplicativos confiáveis da política pai são exibidos nas políticas filho em uma exibição somente leitura. Não é possível alterar ou excluir aplicativos confiáveis da política pai
9. Marque a caixa de seleção **Permitir a edição de aplicativos locais confiáveis** se deseja permitir que o usuário crie uma lista local de aplicativos confiáveis. Dessa forma, um usuário pode criar sua própria lista local de aplicativos confiáveis, além da lista geral de aplicativos confiáveis gerada na política. Um administrador pode usar o Kaspersky Security Center para exibir, adicionar, editar ou excluir itens da lista nas propriedades do computador.

   Se a caixa de seleção estiver desmarcada, o usuário poderá acessar apenas a lista geral de aplicativos confiáveis gerada na política. Além disso, caso a caixa de seleção esteja desmarcada, o Kaspersky Embedded Systems Security ocultará a lista consolidada de aplicativos confiáveis na interface do usuário do aplicativo.

10. Marque a caixa de seleção **Não verificar a atividade dos arquivos dos processos especificados** para ignorar a verificação das operações do arquivo para processos confiáveis.
11. Clique em **Adicionar** e selecione uma ação:

    - **Categoria**. É possível agrupar aplicativos confiáveis em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione pelo menos um aplicativo confiável para ela.
    - **Nova exclusão**. O Kaspersky Embedded Systems Security adiciona um novo aplicativo confiável à raiz da lista.

- **Nova exclusão para a categoria selecionada**. Para adicionar um novo aplicativo confiável a uma categoria específica, selecione uma categoria.
- **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Embedded Systems Security, é possível adicionar aplicativos da lista de aplicativos confiáveis predefinidos.

12. Na janela aberta, marque a caixa de seleção **Use o caminho inteiro do processo no disco para saber se é confiável** e insira o caminho para determinar se o processo é confiável.

    O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:

    > O Kaspersky Embedded Systems Security não é compatível com a variável de ambiente `%userprofile%` ao gerar uma lista de aplicativos confiáveis no console do Kaspersky Security Center. Para aplicar a entrada em todas as contas de usuários, é possível utilizar o caractere * (por exemplo, `C:\Users\*\Documents\File.exe`). Quando adicionar uma nova variável de ambiente, é necessário reiniciar o aplicativo.

13. Defina as configurações avançadas para o aplicativo confiável (consulte a tabela abaixo).
14. Clique **OK**.

    O novo aplicativo confiável será adicionado à lista. Você pode excluir um aplicativo da zona confiável a qualquer momento usando a caixa de seleção na coluna **Ação**.

15. Salvar alterações.

Como adicionar um aplicativo à lista confiável a partir do Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e selecione **Zona confiável** por meio do menu de contexto do nó.

   A janela **Configurar a Zona confiável** é aberta.

2. Na seção **Exclusões**, clique no botão **Configurações** ao lado do bloco **Aplicativos confiáveis**.
3. Clique em **Adicionar** e selecione uma ação:
   - **Categoria**. É possível agrupar aplicativos confiáveis em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione pelo menos um aplicativo confiável para ela.
   - **Nova exclusão**. O Kaspersky Embedded Systems Security adiciona um novo aplicativo confiável à raiz da lista.
   - **Nova exclusão para a categoria selecionada**. Para adicionar um novo aplicativo confiável a uma categoria específica, selecione uma categoria.
   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Embedded Systems Security, é possível adicionar aplicativos da lista de aplicativos confiáveis predefinidos.
4. Selecione um arquivo da lista ou insira o caminho para o arquivo executável do aplicativo confiável.

   O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:

O Kaspersky Embedded Systems Security é compatível com variáveis de ambiente. O Kaspersky Endpoint Security é compatível com variáveis de ambiente e converte o caminho para a interface local do aplicativo. Em outras palavras, se o caminho do arquivo `%userprofile%\Documents\File.exe` for inserido, um registro `C:\Users\Fred123\Documents\File.exe` é adicionado na interface local do aplicativo para o usuário Fred123. Consequentemente, o Kaspersky Embedded Systems Security ignora o programa confiável `File.exe` para outros usuários. Para aplicar a entrada em todas as contas de usuários, é possível utilizar o caractere `*` (por exemplo, `C:\Users\*\Documents\File.exe`).

Quando adicionar uma nova variável de ambiente, é necessário reiniciar o aplicativo.

5. Defina as configurações avançadas para o aplicativo confiável (consulte a tabela abaixo).
6. Clique **OK**.

   O novo aplicativo confiável será adicionado à lista. Você pode excluir um aplicativo da zona confiável a qualquer momento usando a caixa de seleção ao lado do nome do objeto.
7. Salvar alterações.

Configurações do aplicativo confiável

Parâmetro	Descrição
Use o caminho inteiro do processo no disco para saber se é confiável	O Kaspersky Embedded Systems Security usa o caminho completo do arquivo para determinar se o processo é confiável.
Use o hash de arquivo do processo para saber se é confiável	O Kaspersky Embedded Systems Security usa o hash do arquivo selecionado para determinar o status de confiança do processo. Se a caixa de seleção for desmarcada, o hash do arquivo não será usado para determinar o status de confiança do processo.
Permitir interação com interface de aplicativo	O Kaspersky Embedded Systems Security bloqueia todas as tentativas de gerenciar serviços de aplicativos a partir de um computador remoto. Se a caixa de seleção for marcada, o aplicativo de acesso remoto tem permissão para gerenciar configurações do Kaspersky Embedded Systems Security pela interface do Kaspersky Embedded Systems Security.
Não monitorar a atividade de aplicativos secundários	O Kaspersky Embedded Systems Security não vai monitorar a atividade de arquivo ou atividade de rede de aplicativos iniciados pelo aplicativo. Você pode aplicar a exclusão recursivamente. Para que o aplicativo não monitore a atividade de toda a cadeia de aplicativos secundários.
Não herdar restrições do processo principal (aplicativo)	As restrições configuradas para o processo pai não serão aplicadas pelo Kaspersky Embedded Systems Security a um processo filho. O processo pai é iniciado por um aplicativo para o qual os direitos do aplicativo e as regras de rede de aplicativos são configurados.
Não verificar a memória do processo	O Kaspersky Embedded Systems Security não verifica a memória do processo.

Criando uma zona confiável local

Agora, o usuário pode criar sua própria zona confiável local para um computador específico. Dessa forma, os usuários podem criar suas próprias listas locais de exclusões de verificação e aplicativos confiáveis, além da zona confiável geral em uma política. Um administrador pode permitir ou bloquear o uso de exclusões locais ou aplicativos locais confiáveis nas configurações da política. Para fazer isso, use as caixas de seleção **Permitir o uso de exclusões locais** e **Permitir a edição de aplicativos locais confiáveis** nas guias **Exclusões de verificação** e **Aplicativos confiáveis** na seção **Zona confiável** da política.

Caso a criação de uma zona confiável local seja permitida por um administrador, o usuário poderá adicionar suas próprias exclusões de verificação e aplicativos confiáveis no Console do Aplicativo. Ao mesmo tempo, o usuário não terá permissão para modificar ou excluir objetos da zona confiável configurada na política. O administrador também poderá visualizar, adicionar, modificar ou excluir itens da lista no console do Kaspersky Security Center caso seja necessário adicionar as exclusões para um computador individual.

O Kaspersky Embedded Systems Security esconde as listas de exclusões de verificação e aplicativos confiáveis no Console do Aplicativo caso a configuração da zona confiável seja bloqueada pelo administrador no console (símbolo de "cadeado fechado") e as exclusões de verificação e aplicativos confiáveis sejam proibidos.

Como adicionar um objeto na zona confiável local no Console de Administração do Kaspersky Security Center

1. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.
2. No espaço de trabalho, selecione a guia **Dispositivos**.
3. Clique duas vezes para abrir a janela de propriedades do computador.
4. Na janela de propriedades do computador, selecione a seção **Aplicativos**.
5. Na lista de aplicativos da Kaspersky instalados no computador, selecione **Kaspersky Embedded Systems Security** e clique duas vezes para abrir as propriedades do aplicativo.
6. Na janela de configurações do aplicativo, selecione **Suplementar** → **Zona confiável** e clique **Configurações**.
7. Na guia **Exclusões de verificação**, faça uma lista de exclusões de verificação locais.

   As regras para criar exclusões de verificação locais são iguais às exclusões gerais. O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:
8. Na guia **Aplicativos confiáveis**, faça uma lista de aplicativos locais confiáveis. Essa ação abre uma janela que contém uma lista dos aplicativos confiáveis locais.

   As regras para adicionar aplicativos na lista de aplicativos locais confiáveis são iguais às regras para adicioná-los na lista geral. O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:
9. Salvar alterações.

Como adicionar um objeto à zona confiável local no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Dispositivos gerenciados**.
2. Clique no nome do computador no qual você deseja permitir que um usuário execute uma ação bloqueada.
3. Selecione a guia **Aplicativos**.

4. Clique em **Kaspersky Embedded Systems Security**.

   Isso abre as configurações locais do aplicativo.

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

6. Na janela de configurações do aplicativo, selecione **Suplementar** → **Zona confiável** e clique **Configurar**.

   A janela **Exclusões e tipos de objetos detectados** é aberta.

7. Na guia **Exclusões de verificação**, faça uma lista de exclusões de verificação locais.

   As regras para criar exclusões locais são iguais às regras para criar exclusões gerais. O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:

8. Na guia **Aplicativos confiáveis**, faça uma lista de aplicativos locais confiáveis.

   As regras para adicionar aplicativos na lista de aplicativos locais confiáveis são iguais às regras para adicioná-los na lista geral. O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:

9. Salvar alterações.

Como criar uma exclusão de verificação local no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e selecione **Zona confiável** por meio do menu de contexto do nó.

   A janela **Configurar a Zona confiável** é aberta.

2. Na seção **Exclusões de verificação e aplicativos confiáveis**, clique no botão **Configurações** ao lado do bloco **Exclusões de verificação locais**.

   O Kaspersky Embedded Systems Security esconde a lista de exclusões de verificação no Console do Aplicativo caso a configuração de exclusões de verificação seja bloqueada pelo administrador no Console de Administração do Kaspersky Security Center (símbolo de "cadeado fechado") e as exclusões de verificação local sejam proibidas (a caixa de seleção **Permitir o uso de exclusões locais** estará desmarcada).

3. Clique em **Adicionar** e selecione uma ação:

   - **Categoria**. É possível agrupar as exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o seu nome e adicione pelo menos uma exclusão de verificação para ela.
   - **Nova exclusão**. O Kaspersky Embedded Systems Security adiciona uma nova exclusão de verificação à raiz da lista.
   - **Nova exclusão para a categoria selecionada**. Para adicionar uma nova exclusão de verificação a uma categoria específica, selecione uma categoria.
   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Embedded Systems Security, é possível adicionar exclusões da lista de exclusões de verificação predefinidas.

4. Selecionar **Nova exclusão** abrirá a janela **Exclusão de verificação**.

5. Para excluir um arquivo ou pasta da verificação, marque a caixa **Arquivo ou pasta**insira o caminho manualmente. Clique no link **Selecionar arquivo ou pasta** para abrir uma janela, e nessa janela, selecione um arquivo ou pasta com um clique em **Procurar**.

   Também é possível inserir o caminho manualmente. O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:

   - O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas.

   - Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

   - O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/`(delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.

     É possível usar máscaras no início, no meio ou no final do caminho do arquivo. Por exemplo, caso queira adicionar uma pasta para todos os usuários nas exclusões, insira a máscara `?:\Users\*\Folder\`.

6. Para excluir uma área predefinida da verificação, marque a caixa de seleção **Escopo predefinido**. Clique no link **selecionar escopo predefinido** para abrir uma janela, e nessa janela, selecione um dos escopos padrão no dispositivo protegido.

7. Para excluir os objetos específicos da verificação, marque a caixa de seleção **Tipo do objeto detectado**. Clique no link **inserir nomes do objeto**, clique no botão **Adicionar**, e na janela exibida, insira o nome do tipo de objeto de acordo com a classificação da Kaspersky Encyclopedia (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

   Você pode usar máscaras com o caractere `?` (substitui qualquer caractere único) e o caractere `*` (substitui qualquer número de caracteres). Por exemplo, se a máscara do `Client*` for especificada, o Kaspersky Embedded Systems Security exclui os objetos `Client-IRC`, `Client-P2P` e `Client-SMTP` das verificações.

8. Para excluir um arquivo individual da verificação, marque a caixa de seleção **Hash do objeto**. Clique no link **inserir hash do objeto** para abrir uma janela, e nessa janela, insira um hash do arquivo.

   Se o arquivo for modificado, o hash do arquivo também será modificado. Se isso acontecer, o arquivo modificado não será adicionado às exclusões.

9. Na seção **Escopo de uso da regra**, selecione os componentes aos quais deseja que a exclusão de verificação se aplique.

10. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

11. Salve as alterações para adicionar a exclusão na lista. É possível desativar a exclusão a qualquer momento usando a caixa de seleção ao lado do objeto.

Como adicionar um aplicativo na lista de aplicativos locais confiáveis no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e selecione **Zona confiável** por meio do menu de contexto do nó.

   A janela **Configurar a Zona confiável** é aberta.

2. Na seção **Exclusões**, clique no botão **Configurações** ao lado do bloco **Aplicativos locais confiáveis**.

   O Kaspersky Embedded Systems Security esconde a lista consolidada de aplicativos confiáveis no Console do Aplicativo caso a configuração de aplicativos confiáveis seja bloqueada pelo administrador no Console de Administração do Kaspersky Security Center (símbolo de "cadeado fechado") e os aplicativos confiáveis locais sejam proibidos (a caixa de seleção **Permitir a edição de aplicativos locais confiáveis** estará desmarcada).

3. Clique em **Adicionar** e selecione uma ação:

   - **Categoria**. É possível agrupar aplicativos confiáveis em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione pelo menos um aplicativo confiável para ela.
   - **Nova exclusão**. O Kaspersky Embedded Systems Security adiciona um novo aplicativo confiável à raiz da lista.
   - **Nova exclusão para a categoria selecionada**. Para adicionar um novo aplicativo confiável a uma categoria específica, selecione uma categoria.
   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Embedded Systems Security, é possível adicionar aplicativos da lista de aplicativos confiáveis predefinidos.

4. Selecionar **Nova exclusão** abrirá a janela **Exclusão de verificação**.

5. Marque a caixa de seleção **Use o caminho inteiro do processo no disco para saber se é confiável** e insira o caminho para o arquivo executável do aplicativo confiável.

   O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara:

   O Kaspersky Embedded Systems Security é compatível com variáveis de ambiente. O Kaspersky Endpoint Security é compatível com variáveis de ambiente e converte o caminho para a interface local do aplicativo. Em outras palavras, se o caminho do arquivo `%userprofile%\Documents\File.exe` for inserido, um registro `C:\Users\Fred123\Documents\File.exe` é adicionado na interface local do aplicativo para o usuário Fred123. Consequentemente, o Kaspersky Embedded Systems Security ignora o programa confiável `File.exe` para outros usuários. Para aplicar a entrada em todas as contas de usuários, é possível utilizar o caractere `*` (por exemplo, `C:\Users\*\Documents\File.exe`).

   Quando adicionar uma nova variável de ambiente, é necessário reiniciar o aplicativo.

6. Na janela de propriedades do aplicativo confiável, defina as configurações avançadas.

7. Salve as alterações para adicionar a exclusão na lista.

Exportar e importar a zona confiável

Uma *zona confiável* é uma lista de objetos e aplicativos configuradas pelo administrador de sistema que o Kaspersky Embedded Systems Security não monitora quando ativado. A zona confiável consiste nas seguintes listas: *exclusões de verificação* e *aplicativos confiáveis*. Em seguida, você pode modificar o arquivo para, por exemplo, adicionar um grande número de exclusões do mesmo tipo. Também é possível usar a função de exportação/importação para fazer backup da lista de exclusões e a lista de aplicativos confiáveis ou para migrar as listas para um servidor diferente.

O aplicativo usa o formato XML para exportar e importar a *lista de exclusões* e os aplicativos confiáveis:

O Kaspersky Embedded Systems Security não é compatível com as listas de exclusão e de aplicativos confiáveis que contenham mais de cinco mil objetos.

Como exportar e importar a zona confiável no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Suplementar** → **Zona confiável** e clique em **Configurações**.
4. Para exportar a lista de regras:
   a. Selecione a guia **Exclusões de verificação**.
   b. Selecione as exclusões que deseja exportar.
      Se você não selecionou nenhuma exclusão, o Kaspersky Embedded Systems Security exportará todas as exclusões.
   c. Clique no ícone da pasta e selecione **Exportar** na lista suspensa.
      Na janela exibida, especifique o nome do arquivo XML para o qual você quer exportar a lista de exclusões e selecione a pasta na qual você quer salvar esse arquivo.
   d. Salvar o arquivo.
5. Para exportar a lista de aplicativos confiáveis:
   a. Selecione a guia **Aplicativos confiáveis**.
      Essa ação abre uma janela que contém uma lista dos aplicativos confiáveis.
   b. Selecione os aplicativos confiáveis que deseja exportar.
      Caso não selecione nenhum aplicativo confiável, o Kaspersky Embedded Systems Security exportará todos os aplicativos confiáveis.
   c. Clique no ícone da pasta e selecione **Exportar** na lista suspensa.

d. Na janela aberta, insira o nome do arquivo XML para o qual deseja exportar a lista de aplicativos confiáveis e selecione a pasta na qual deseja salvar esse arquivo.

e. Salvar o arquivo.

O Kaspersky Embedded Systems Security exporta toda a lista de regras para o arquivo XML.

6. Para importar a lista de exclusões:

a. Selecione a guia **Exclusões de verificação**.

Aparecerá uma janela com uma lista de exclusões.

b. Clique no ícone da pasta e selecione **Importar** na lista suspensa.

c. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de exclusões.

d. Abra o arquivo.

Se o computador já tiver uma lista de exclusões, o Kaspersky Embedded Systems Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

7. Para importar a lista de aplicativos confiáveis:

a. Selecione a guia **Aplicativos confiáveis**.

Essa ação abre uma janela que contém uma lista dos aplicativos confiáveis.

b. Clique **Importar**.

c. Na janela exibida, selecione o arquivo XML a partir do qual deseja importar a lista de aplicativos confiáveis.

d. Abra o arquivo.

Se o computador já tiver uma lista de aplicativos confiáveis, o Kaspersky Embedded Systems Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

8. Salvar alterações.

Como exportar e importar a zona confiável no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

A janela de propriedades da política é exibida.

3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Suplementar** → **Zona confiável** e clique no botão **Configurar**.
5. Para exportar a lista de regras:

a. Na guia **Exclusões de verificação e aplicativos confiáveis**, selecione as exclusões que deseja exportar.

b. Clique nos três pontos e selecione **Exportar**.

c. Confirme que deseja exportar apenas as exclusões selecionadas ou exportar toda a lista de exclusões.

O Kaspersky Embedded Systems Security exporta toda a lista de regras para o arquivo XML.

6. Para exportar a lista de aplicativos confiáveis:

a. Na guia **Exclusões de verificação e aplicativos confiáveis**, selecione os aplicativos que deseja exportar.

b. Clique nos três pontos e selecione **Exportar**.

c. Confirme se deseja exportar apenas os aplicativos selecionados ou exportar a lista inteira.

O Kaspersky Embedded Systems Security exporta toda a lista de regras para o arquivo XML.

7. Para importar a lista de exclusões:

a. Na guia **Exclusões de verificação e aplicativos confiáveis**, clique em **Importar da versão anterior** caso queira importar a lista de exclusões de um arquivo XML criado na versão 3.4 ou anterior do aplicativo.

Caso esteja importando as regras de um arquivo XML criado na versão 4.0 ou posterior, clique em **Importar**.

b. Se o computador já tiver uma lista de exclusões, o Kaspersky Embedded Systems Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

c. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de exclusões.

d. Clique **Importar**.

8. Para importar a lista de aplicativos confiáveis:

a. Na guia **Exclusões de verificação e aplicativos confiáveis**, clique em **Importar da versão anterior** caso queira importar a lista de aplicativos confiáveis de um arquivo XML criado na versão 3.4 ou anterior do aplicativo.

Caso esteja importando os aplicativos confiáveis de um arquivo XML criado na versão 4.0 ou posterior, clique em **Importar**.

b. Se o computador já tiver uma lista de aplicativos confiáveis, o Kaspersky Embedded Systems Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

c. Na janela exibida, selecione o arquivo XML a partir do qual deseja importar a lista de aplicativos confiáveis.

d. Clique **Importar**.

9. Salvar alterações.

Como exportar ou importar a zona confiável no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e selecione **Zona confiável** por meio do menu de contexto do nó.

A janela **Configurar a Zona confiável** é aberta.

2. Para exportar a lista de exclusões ou aplicativos confiáveis:

   a. Na seção **Exclusões**, clique no botão **Configurações** ao lado dos blocos **Exclusões de verificação** ou **Aplicativos confiáveis**.

   b. Selecionar as exclusões ou aplicativos confiáveis que deseja exportar.

   c. Clique no ícone da pasta e selecione **Exportar**.

   d. Na janela aberta, insira o nome do arquivo XML para o qual deseja exportar a lista de exclusões ou aplicativos confiáveis e selecione a pasta na qual deseja salvar esse arquivo.

   e. Salvar o arquivo.

      O Kaspersky Embedded Systems Security exporta toda a lista de regras para o arquivo XML.

3. Para importar uma lista de exclusões ou aplicativos confiáveis:

   a. Na seção **Exclusões**, clique no botão **Configurações** ao lado dos blocos **Exclusões de verificação** ou **Aplicativos confiáveis**.

   b. Selecione as exclusões ou aplicativos confiáveis que deseja importar.

   c. Clique no ícone da pasta e selecione **Exportar**.

   d. Na janela exibida, selecione o arquivo XML a partir do qual deseja importar a lista de exclusões ou aplicativos confiáveis.

   e. Abra o arquivo.

      Se o computador já tiver uma lista de exclusões, o Kaspersky Embedded Systems Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

4. Salvar alterações.

Usar armazenamento de certificado de sistema confiável

O uso do armazenamento de certificado de sistema permite excluir aplicativos assinados por uma assinatura digital confiável de verificações de vírus. O Kaspersky Embedded Systems Security atribui automaticamente esses aplicativos ao grupo *Confiável*.

Para começar a usar o armazenamento de certificado de sistema confiável:

Como configurar o uso de um armazenamento de certificado de sistema confiável no Kaspersky Security Center Administration Console

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Suplementar** → **Zona confiável** e clique em **Configurações**.

4. Selecione a guia **Armazenamento de certificados de sistema confiáveis**.

5. Marque a caixa de seleção **Usar armazenamento de certificados de sistema confiáveis**, e na lista suspensa, selecione o armazenamento do sistema desejado no Kaspersky Embedded Systems Security a ser considerado confiável.

6. Salvar alterações.

Como configurar o uso de um armazenamento de certificado de sistema confiável no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Vá para **Suplementar** → **Zona confiável** e clique no botão **Configurar**.

5. Selecione a guia **Armazenamento de certificados de sistema confiáveis**.

6. Marque a caixa de seleção **Usar armazenamento de certificados de sistema confiáveis**, e na lista suspensa, selecione o armazenamento do sistema desejado no Kaspersky Embedded Systems Security a ser considerado confiável.

7. Salvar alterações.

Como configurar o uso de um armazenamento de certificado de sistema confiável no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e selecione **Zona confiável** por meio do menu de contexto do nó.

   A janela **Configurar a Zona confiável** é aberta.

2. Em **Armazenamento de certificados de sistema confiáveis**, marque a caixa de seleção **Usar armazenamento de certificados de sistema confiáveis**, e na lista suspensa, selecione o armazenamento do sistema desejado no Kaspersky Embedded Systems Security a ser considerado confiável.

3. Salvar alterações.

Proteção de Arquivos em Tempo Real

O componente Proteção de Arquivos em Tempo Real do Kaspersky Embedded Systems Security verifica os seguintes objetos do dispositivo protegido assim que acessados:

- Arquivos
- Fluxos de dados alternativos do NTFS.
- Registros mestre de inicialização e setores de inicialização em discos rígidos locais e dispositivos externos.
- Arquivos de contêiner do Windows Server 2016 e Windows Server 2019.

Quando um aplicativo grava ou lê um arquivo no dispositivo protegido, o Kaspersky Embedded Systems Security 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 salvará uma cópia criptografada do arquivo fonte na pasta de Backup.

O Kaspersky Embedded Systems Security intercepta as operações de arquivos executadas em contêineres do Windows Server 2016 e Windows Server 2019.

Um *contêiner* é um ambiente isolado no qual um aplicativo pode ser executado sem interagir diretamente com o sistema operacional. Caso o contêiner esteja localizado no escopo de proteção do componente, o Kaspersky Embedded Systems Security verificará os arquivos do contêiner, que estão sendo acessados pelos usuários, em busca de ameaças para o computador. Quando uma ameaça é detectada, o aplicativo tenta desinfectar o contêiner. Caso a desinfecção seja bem-sucedida, o contêiner continuará funcionando. Caso a desinfecção falhe, o contêiner será desligado.

O Kaspersky Embedded Systems Security também detecta malware em processos executados sob o subsistema Windows para Linux®. Para esses processos, o componente 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, o componente 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 lista dos recursos de arquivos do dispositivo que o Kaspersky Embedded Systems Security pode monitorar.

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 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 nós ou itens selecionados na lista de recursos de arquivo (o nível de segurança é alterado para **Personalizado**).

Escopos da proteção predefinidos

A 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 abrange os seguintes escopos de proteção predefinidos:

- **Discos rígidos locais**. O Kaspersky Embedded Systems Security protege arquivos nos discos rígidos do dispositivo.
- **Unidades removíveis**. O Kaspersky Embedded Systems Security 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 verifica os arquivos gravados em pastas de redes ou lidos nelas por aplicativos em execução no dispositivo. O Kaspersky Embedded Systems Security não protege os arquivos quando eles são acessados por aplicativos de outros dispositivos protegidos.

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.

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 (Universal Naming Convention).

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**, **Proteção máxima** e **Informar**. 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 caso a rede tenha medidas de segurança adicionais nos dispositivos protegidos, como firewalls e políticas de segurança existentes, além de usar o Kaspersky Embedded Systems Security nos dispositivos e estações de trabalho 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.

Informar

O nível de segurança **Informar** é recomendado caso haja muitos computadores com potencial de infecção na rede corporativa e o bloqueio desses computadores possa interromper significativamente a operação da organização.

Níveis de segurança predefinidos e valores de configurações correspondentes

Opções	Nível de segurança			
Desempenho máximo	Recomendado	Proteção máxima	Informar	
Proteção de objetos	Objetos verificados de acordo com a lista de extensões especificada no banco de dados antivírus	Objetos verificados por formato	Objetos verificados por formato	Objetos verificados por formato
Verificar somente arquivos novos e alterados	Ativado	Ativado	Desativado	Ativado
Verificação de arquivos compostos	Desativado	Verificar arquivos nos formatos do Microsoft Office	Verificar arquivos nos formatos do Microsoft Office	Verificar arquivos nos formatos do Microsoft Office
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	Informações
Aplicar a ação aos tipos de objeto selecionados	Desativado	Desativado	Desativado	Desativado
Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado	Desativado	Desativado	Ativado	Desativado
Os objetos críticos do sistema são arquivos necessários para a operação do sistema operacional e do Kaspersky Embedded Systems Security. Esses arquivos não podem ser excluídos. Os processos associados a esses objetos não podem ser encerrados.				
Descompactar os arquivos compostos em segundo plano maiores que (MB)				

Opções	Nível de segurança			
Parar a verificação se demorar mais que (s)	60 s	60 s	60 s	60 s
Não verificar objetos compostos com mais de (MB)	8 MB	8 MB	Não definido	8 MB
Usar a tecnologia iSwift	Ativado	Ativado	Ativado	Ativado
Usar a tecnologia iChecker	Ativado	Ativado	Ativado	Ativado

Extensões de arquivos verificadas por padrão na tarefa de Proteção de Arquivos em Tempo Real

O Kaspersky Embedded Systems Security 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?.*

Configuração da tarefa de Proteção de Arquivos em Tempo Real

Por padrão, o componente Proteção de Arquivos em Tempo Real usa as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Configurações padrão do componente de Proteção de Arquivos em Tempo Real

Parâmetro	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.

Parâmetro	Valor padrão	Descrição
Modo de proteção de 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 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.
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 criará e iniciará uma tarefa de verificação de áreas críticas.
Interromper o contêiner caso a desinfecção falhe	Aplicada.	O aplicativo pode não ter direitos de leitura e gravação suficientes para o objeto detectado. Nesse caso, não é possível desinfectar ou excluir o objeto detectado. Se essa caixa de seleção estiver marcada, o aplicativo bloqueia o objeto detectado e interrompe o contêiner. Se essa caixa de seleção estiver desmarcada, o aplicativo apenas bloqueia o objeto detectado.
Não verificar as operações executadas nos contêineres do Windows	Aplicada.	Caso essa caixa de seleção esteja marcada, o aplicativo verificará o contêiner somente quando ele for iniciado. Se a caixa de seleção estiver desmarcada, o aplicativo verifica o contêiner continuamente em tempo real.

Como ativar as verificações de vírus de arquivos no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção do Computador em Tempo Real**.
4. Na seção **Configurações de Proteção de Arquivos em Tempo Real**, clique no botão **Configurações**.
5. Marque a caixa de seleção **Proteção de Arquivos em Tempo Real**.
6. No bloco **Modo de proteção de objetos**, na guia **Geral**, selecione o modo de operação de Proteção de Arquivos em Tempo Real:
   - **Modo inteligente**. O Kaspersky Embedded Systems Security 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 verifica o objeto novamente somente após o objeto ter sido salvo pelo processo pela última vez.
   - **Ao acessar e modificar**. O Kaspersky Embedded Systems Security verifica um objeto quando ele é aberto e novamente após ele ser salvo, caso tenha sido modificado. Esta opção é selecionada por padrão.
   - **Ao acessar**. O Kaspersky Embedded Systems Security verifica todos os objetos quando são abertos para a leitura, execução ou modificação.
   - **Ao executar**. O Kaspersky Embedded Systems Security verificará um arquivo apenas quando for acessado para execução.
7. Desmarque ou marque a caixa de seleção **Usar a análise heurística**.

8. Selecione ou desmarque a caixa de seleção **Bloquear o acesso a recursos de rede compartilhados para sessões que exibem atividade maliciosa**.

9. Desmarque ou marque a caixa de seleção **Iniciar a verificação de áreas críticas quando uma infecção ativa for detectada**.

   Caso a caixa de seleção esteja marcada, quando a infecção ativa for detectada, o Kaspersky Embedded Systems Security executará a tarefa de *Verificação de áreas críticas*. A caixa de seleção é marcada por padrão.

10. Especifique as configurações de verificação das operações com arquivos executadas em contêineres do Windows.

11. Salvar alterações.

Como ativar as verificações de vírus de arquivos no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Vá para **Proteção do Computador em Tempo Real** → **Proteção de Arquivos em Tempo Real** e clique no botão **Configurar**.

5. Marque a caixa de seleção **Ativar Proteção de arquivos em tempo real**.

6. No bloco **Modo de proteção de objetos**, na guia **Geral**, selecione o modo de operação de Proteção de Arquivos em Tempo Real:

   - **Modo inteligente**. O Kaspersky Embedded Systems Security 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 verifica o objeto novamente somente após o objeto ter sido salvo pelo processo pela última vez.

   - **Ao acessar e modificar**. O Kaspersky Embedded Systems Security verifica um objeto quando ele é aberto e novamente após ele ser salvo, caso tenha sido modificado. Esta opção é selecionada por padrão.

   - **Ao acessar**. O Kaspersky Embedded Systems Security verifica todos os objetos quando são abertos para a leitura, execução ou modificação.

   - **Ao executar**. O Kaspersky Embedded Systems Security verificará um arquivo apenas quando for acessado para execução.

7. Desmarque ou marque a caixa de seleção **Usar a análise heurística**.

8. Selecione ou desmarque a caixa de seleção **Bloquear o acesso a recursos de rede compartilhados para sessões que exibem atividade maliciosa**.

9. Desmarque ou marque a caixa de seleção **Iniciar a verificação de áreas críticas quando uma infecção ativa for detectada**.

   Caso a caixa de seleção esteja marcada, quando a infecção ativa for detectada, o Kaspersky Embedded Systems Security executará a tarefa de *Verificação de áreas críticas*. A caixa de seleção é marcada por padrão.

10. Especifique as configurações de verificação das operações com arquivos executadas em contêineres do Windows.

11. Salvar alterações.

Como ativar as verificações de vírus de arquivos no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Proteção do Computador em Tempo Real → Proteção de arquivos em tempo real**.

2. no painel de resultados do node **Proteção de arquivos em tempo real**, clique no link **Propriedades**.

   A janela **Propriedades: Proteção de arquivos em tempo real** é aberta.

3. Marque a caixa de seleção **Proteção de arquivos em tempo real**.

4. No bloco **Modo de proteção de objetos**, na guia **Geral**, selecione o modo de operação de Proteção de Arquivos em Tempo Real:

   - **Modo inteligente**. O Kaspersky Embedded Systems Security 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 verifica o objeto novamente somente após o objeto ter sido salvo pelo processo pela última vez.

   - **Ao acessar e modificar**. O Kaspersky Embedded Systems Security verifica um objeto quando ele é aberto e novamente após ele ser salvo, caso tenha sido modificado. Esta opção é selecionada por padrão.

   - **Ao acessar**. O Kaspersky Embedded Systems Security verifica todos os objetos quando são abertos para a leitura, execução ou modificação.

   - **Ao executar**. O Kaspersky Embedded Systems Security verificará um arquivo apenas quando for acessado para execução.

5. Desmarque ou marque a caixa de seleção **Usar a análise heurística**.

6. Selecione ou desmarque a caixa de seleção **Bloquear o acesso a recursos de rede compartilhados para sessões que exibem atividade maliciosa**.

7. Desmarque ou marque a caixa de seleção **Iniciar a verificação de áreas críticas quando uma infecção ativa for detectada**.

   Caso a caixa de seleção esteja marcada, quando a infecção ativa for detectada, o Kaspersky Embedded Systems Security executará a tarefa de *Verificação de áreas críticas*. A caixa de seleção é marcada por padrão.

8. Especifique as configurações de verificação das operações com arquivos executadas em contêineres do Windows.

9. Salvar alterações.

Configurando o escopo de proteção para o componente de Proteção de Arquivos em Tempo Real

Por padrão, o componente 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 para que sejam definidos como configurações comuns para todo o escopo da proteção ou como configurações diferentes para itens individuais na lista de recursos de arquivos do dispositivo.

Caso o mesmo objeto esteja incluído em várias entradas do escopo de proteção e essas entradas tiverem níveis de segurança diferentes, a última regra na lista terá prioridade. Por exemplo, considere um escopo de proteção que inclua duas entradas: **Todos os discos rígidos** (nível de segurança **Informar**) e `*\Users\*\Downloads\*` (nível de segurança **Personalizado**). O aplicativo verifica os discos rígidos de acordo com o nível Informar, exceto a pasta `Downloads`. O aplicativo verifica a pasta `Downloads` de acordo com as configurações especificadas manualmente porque essa entrada é a última na lista do escopo de proteção.

Para definir as configurações de segurança do node selecionado manualmente:

Como configurar o escopo de proteção para a Proteção de Arquivos em Tempo Real no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção do Computador em Tempo Real**.

4. Na seção **Proteção de Arquivos em Tempo Real**, clique no botão **Configurações**.

5. Selecione a guia **Escopo de proteção**.

6. Na lista de recursos de arquivos do dispositivo protegido, selecione os itens para os quais deseja definir um nível de segurança predefinido.

7. Se o arquivo compartilhado não estiver na lista, adicione-o manualmente:

   a. Clique **Adicionar**.

   b. Use a árvore de pastas para especificar o caminho para o objeto desejado ou insira-o no campo **Objeto**.

Se necessário, use caracteres especiais para inserir a máscara do caminho do objeto:

- O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas.

- Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

- O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/`(delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.

O objeto **Este PC** na lista de recursos do computador inclui os seguintes objetos: **Todos os discos rígidos**, **Todas as unidades de rede** e **Todas as unidades removíveis**.

c. Clique **OK**.

8. Verifique e confirme se o nó ou item selecionado foi incluído no escopo da proteção.

9. Especifique um nível de segurança predefinido para o escopo de proteção selecionado clicando em **Configurar**. Por padrão, as mesmas configurações de segurança são aplicadas em todo o escopo de proteção. Estas configurações correspondem ao nível de segurança predefinido **Recomendado**. Também é possível editar as configurações de segurança padrão.

10. Salvar alterações.

Como configurar o escopo de proteção para a Proteção de Arquivos em Tempo Real no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Vá para **Proteção do Computador em Tempo Real** → **Proteção de Arquivos em Tempo Real** e clique no botão **Configurar**.

5. Selecione a guia **Escopo de proteção**.

6. Na lista de recursos de arquivos do dispositivo protegido, selecione os itens para os quais deseja definir um nível de segurança predefinido.

7. Se o arquivo compartilhado não estiver na lista, adicione-o manualmente:

   a. Clique **Adicionar**.

   b. Na lista **Tipo de objeto**, selecione uma opção:

      Para a opção **Máscara**, use caracteres especiais para inserir a máscara do caminho do objeto:

      - O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas.

      - Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

      - O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/`(delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.

      O objeto **Este PC** na lista de recursos do computador inclui os seguintes objetos: **Todos os discos rígidos**, **Todas as unidades de rede** e **Todas as unidades removíveis**.

   c. Clique **OK**.

8. Verifique e confirme se o recurso de arquivo selecionado está incluído no escopo de proteção com o uso do botão de alternância ao lado do item da lista.

9. Especifique um nível de segurança predefinido para o escopo de proteção selecionado clicando em **Editar**. Por padrão, as mesmas configurações de segurança são aplicadas em todo o escopo de proteção. Estas configurações correspondem ao nível de segurança predefinido **Recomendado**. Também é possível editar as configurações de segurança padrão.

10. Salvar alterações.

Como configurar o escopo de proteção para a Proteção de Arquivos em Tempo Real no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Proteção do Computador em Tempo Real → Proteção de Arquivos em Tempo Real**.

2. no painel de resultados do node **Proteção de Arquivos em Tempo Real**, clique no link **Configurar o escopo de proteção**.

   A janela **Propriedades: Proteção de Arquivos em Tempo Real** é aberta.

3. Na lista de recursos de arquivos do dispositivo protegido, selecione os itens para os quais deseja definir um nível de segurança predefinido.

4. Se o arquivo compartilhado não estiver na lista, adicione-o manualmente:

   a. Clique **Adicionar**.

   b. Use a árvore de pastas para especificar o caminho para o objeto desejado ou insira-o no campo **Objeto**.

      Se necessário, use caracteres especiais para inserir a máscara do caminho do objeto:

      - O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas.

      - Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

      - O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/`(delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.

      O objeto **Este PC** na lista de recursos do computador inclui os seguintes objetos: **Todos os discos rígidos**, **Todas as unidades de rede** e **Todas as unidades removíveis**.

   c. Clique **OK**.

5. Verifique e confirme se o nó ou item selecionado foi incluído no escopo da proteção.

6. Especifique um nível de segurança predefinido para o escopo de proteção selecionado clicando em **Configurar**. Por padrão, as mesmas configurações de segurança são aplicadas em todo o escopo de proteção. Estas configurações correspondem ao nível de segurança predefinido **Recomendado**. Também é possível editar as configurações de segurança padrão.

7. Salvar alterações.

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.

Como definir manualmente as configurações de segurança no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção do Computador em Tempo Real**.
4. Na seção **Proteção de Arquivos em Tempo Real**, clique no botão **Configurações**.
5. Na janela **Proteção de Arquivos em Tempo Real**, acesse a guia **Escopo de proteção**.
6. Selecione o recurso para o qual deseja definir as configurações de segurança.
7. Clique **Configurar**.
8. Na janela que é aberta, selecione o nível de segurança necessário e clique em **Configurações**..
9. Na guia **Geral**, defina as seguintes configurações:
   - Objetos que devem ser incluídos no escopo de proteção:
     - Todos os objetos
     - Objetos verificados por formato
     - Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus
   - Na seção **Otimização**, marque ou desmarque a caixa de seleção Verificar somente arquivos novos e alterados.
   - Na seção **Verificação de arquivos compostos**, especifique os objetos compostos que deseja incluir no escopo da verificação:
     - Verificar arquivos comprimidos
     - Verificar pacotes de distribuição
     - Verificar arquivos de formatos do Microsoft Office
     - Verificar arquivos de formato de e-mail
10. Na guia **Ações**, defina as seguintes configurações:
    - Selecione a ação a ser executada em objetos infectados e outros objetos detectados:
      - Informar
      - Bloquear
      - **Executar ação adicional**

Selecionar ação da lista suspensa:

- **Desinfectar**
- **Desinfectar e excluir se a desinfecção falhar**
- **Excluir**
- **Recomendado**

- Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:

  a. Desmarque ou marque a caixa de seleção **Aplicar a ação aos tipos de objetos selecionados**.

  b. Clique em **Configurações** e selecione os tipos de objetos que serão detectados.

- Configurar as ações em arquivos compostos que não estejam disponíveis para modificação: desmarque ou marque a caixa de seleção **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado**.

11. Na guia **Desempenho**, defina as seguintes configurações:

- **Descompactar os arquivos compostos em segundo plano maiores que (MB)**
- **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. Salvar as novas configurações de segurança.

Como definir manualmente as configurações de segurança no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção do Computador em Tempo Real** → **Proteção de Arquivos em Tempo Real** e clique no botão **Configurar**.
5. Selecione a guia **Escopo de proteção**.

6. Execute uma das seguintes ações:

   - Clique no botão **Adicionar** para adicionar uma nova regra e especificar suas configurações de segurança.
   - Selecione uma regra existente e clique no botão **Editar**.

   A janela **Editar escopo** é aberta.

7. Defina o botão de alternância para **Ativo**.
8. Selecione um nível de segurança e especifique as configurações de segurança conforme seja necessário.
9. Na seção **Modo de proteção de objetos**, especifique o tipo de objeto que deseja incluir no escopo de proteção:

   - **Todos os objetos**
   - **Objetos verificados por formato**
   - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**

10. Na seção **Otimização**, 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:

    - **Verificar arquivos compactados**
    - **Verificar pacotes de distribuição**
    - **Verificar arquivos de formatos do Microsoft Office**
    - **Verificar arquivos de formato de e-mail**

12. Selecione a ação a ser executada em objetos infectados e outros objetos detectados:

    - **Informar**
    - **Bloquear**
    - **Executar ação adicional**

      Selecionar ação da lista suspensa:

      - **Desinfectar**
      - **Desinfectar e excluir se a desinfecção falhar**
      - **Excluir**
      - **Recomendado**

13. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:

    a. Desmarque ou marque a caixa de seleção **Aplicar a ação aos tipos de objetos selecionados**.

    b. Caso a caixa de seleção esteja marcada, clique em **Configurações** e selecione os tipos de objetos que serão detectados.

14. Configurar as ações em arquivos compostos que não estejam disponíveis para modificação: desmarque ou marque a caixa de seleção **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado**.

15. Na seção **Otimização**, defina as seguintes configurações:

    - **Descompactar arquivos compostos em segundo plano**
    - **Parar a verificação se demorar mais que (s)**
    - **Não verificar objetos compostos com mais de (MB)**
    - **Usar a tecnologia iSwift**
    - **Usar a tecnologia iChecker**

16. Salvar as novas configurações de segurança.

Como definir as configurações de segurança manualmente no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Proteção do Computador em Tempo Real → Proteção de Arquivos em Tempo Real**.

2. no painel de resultados do node **Proteção de Arquivos em Tempo Real**, clique no link **Configurar o escopo de proteção**.

   A janela **Propriedades: Proteção de Arquivos em Tempo Real** é aberta.

3. Selecione o recurso para o qual deseja definir as configurações de segurança.

4. Clique **Configurar**.

5. Na janela que é aberta, selecione o nível de segurança necessário e clique em **Configurações**..

6. Na guia **Geral**, defina as seguintes configurações:

- Objetos que devem ser incluídos no escopo de proteção:
  - **Todos os objetos**. O Kaspersky Embedded Systems Security verifica todos os objetos.
  - **Objetos verificados por formato**. O Kaspersky Embedded Systems Security verificará somente objetos infectáveis com base no formato do arquivo. A lista de formatos é compilada pela Kaspersky. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security.
  - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**. O Kaspersky Embedded Systems Security verificará somente objetos infectáveis com base na extensão do arquivo. A lista de extensões é compilada pela Kaspersky. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security.
- Na seção **Otimização**, marque ou desmarque a caixa de seleção **Proteger somente arquivos novos e modificados**.
- Na seção **Verificação de arquivos compostos**, especifique os objetos compostos que deseja incluir no escopo da verificação:
  - **Verificar arquivos comprimidos**. Verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos compactados. O aplicativo verifica os arquivos por extensão e formato. Ao verificar os arquivos, o aplicativo executa uma descompactação recursiva. Isso permite detectar ameaças em arquivos multinível (arquivo dentro de arquivo).
  - **Verificar pacotes de distribuição**. Esta caixa de seleção ativa/desativa a verificação de pacotes de distribuição de terceiros.
  - **Verificar arquivos de formatos do Microsoft Office**. Verifica arquivos do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Arquivos de formato do Office também incluem objetos OLE. O Kaspersky Embedded Systems Security verifica arquivos em formato do Office com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.
  - **Verificar arquivos de formato de e-mail**.

7. Na guia **Ações**, defina as seguintes configurações:

- Selecione a ação a ser executada em objetos infectados e outros objetos detectados:
  - **Informar**.
  - **Bloquear**.
  - **Executar ação adicional**.

    Selecionar ação da lista suspensa:
    - **Desinfectar**
    - **Desinfectar e excluir se a desinfecção falhar**
    - **Excluir**.
    - **Recomendado**.

- Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:

  a. Desmarque ou marque a caixa de seleção **Aplicar a ação aos tipos de objeto selecionados**.

  b. Clique em **Configurações** e selecione os tipos de objetos que serão detectados.

- Configurar as ações em arquivos compostos que não estejam disponíveis para modificação: desmarque ou marque a caixa de seleção **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado**.

8. Na guia **Desempenho**, defina as seguintes configurações:

   - **Descompactar os arquivos compostos em segundo plano maiores que (MB)**.
   - **Parar a verificação se demorar mais que (s)**.
   - **Não verificar objetos compostos com mais de (MB)**.
   - **Usar a tecnologia iSwift**.
   - **Usar a tecnologia iChecker**.

9. Salvar as novas configurações de segurança.

Verificação de contêineres

O *contêiner* é um ambiente isolado no qual um aplicativo pode ser executado sem interagir diretamente com o sistema operacional. O uso de contêineres envolve os seguintes riscos:

- Os hackers podem explorar vulnerabilidades de conteinerização para comprometer os aplicativos dentro do contêiner.
- Os hackers podem explorar uma configuração insegura do ambiente do contêiner para obter acesso não autorizado aos dados no computador ou comprometer a integridade do sistema.
- Um ataque bem-sucedido em um contêiner pode permitir que um hacker obtenha acesso aos dados no computador.
- Os hackers podem explorar as vulnerabilidades de rede para interceptar o tráfego de rede.

O Kaspersky Embedded Systems Security é uma ferramenta externa para detectar atividades maliciosas dentro de contêineres. Isso permite manter o desempenho dos contêineres e evita conflitos com outros aplicativos dentro do contêiner. A instalação do Kaspersky Embedded Systems Security dentro do contêiner não é compatível.

Além de fornecer segurança de contêiner, o Kaspersky Embedded Systems Security permite gerenciar aplicativos dentro de contêineres com o uso do Controle de Inicialização de Aplicativos. O Controle de Inicialização de Aplicativos é configurado para os contêineres da mesma forma que para os aplicativos instalados no computador. O Monitor de integridade do sistema também tem suporte para contêineres.

Requisitos do contêiner

- O contêiner deve ser um contêiner do Docker. Outras ferramentas de conteinerização não são compatíveis.
- O contêiner deve ser executado no modo de isolamento do processo. O modo de isolamento do Hyper-V não é compatível.
- O contêiner deve ser colocado em um servidor Windows Server 2016, 2019 ou 2022 (Docker Host).
- O contêiner deve incluir uma imagem do Windows (Docker Image). Os Windows 10 e 11 não são compatíveis. As imagens do Linux não são compatíveis.
- A verificação de contêineres executados no modo WSL2 – Windows Subsystem for Linux v2 (Docker Wine) não é compatível.

Ação ao detectar ameaças

Caso uma ameaça seja detectada dentro de um contêiner, o aplicativo aplicará a ação selecionada para o componente Proteção de Arquivos em Tempo Real. A verificação de contêineres tem configurações adicionais (consulte as instruções abaixo). Se uma ameaça for detectada, o aplicativo bloqueia a atividade maliciosa e executa a ação selecionada (por exemplo, tenta desinfectar o objeto). O Kaspersky Embedded Systems Security poderá interromper o contêiner caso ele não consiga desinfectar o objeto detectado. Por padrão, a interrupção do contêiner está ativada.

Como configurar a verificação de contêineres no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção do Computador em Tempo Real**.
4. Na seção **Proteção de Arquivos em Tempo Real**, clique no botão **Configurações**.
5. No bloco **Verificar as operações executadas nos contêineres do Windows**, defina as configurações da verificação de contêiners:
   - **Interromper o contêiner caso a desinfecção falhe**. O aplicativo pode não ter direitos de leitura e gravação suficientes para o objeto detectado. Nesse caso, não é possível desinfectar ou excluir o objeto detectado. Se essa caixa de seleção estiver marcada, o aplicativo bloqueia o objeto detectado e interrompe o contêiner. Se essa caixa de seleção estiver desmarcada, o aplicativo apenas bloqueia o objeto detectado.
   - **Não verificar as operações executadas nos contêineres do Windows**. Caso essa caixa de seleção esteja marcada, o aplicativo verificará o contêiner somente quando ele for iniciado. Se a caixa de seleção estiver desmarcada, o aplicativo verifica o contêiner continuamente em tempo real.
6. Salvar as novas configurações de segurança.

Como configurar a verificação de contêineres no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção do Computador em Tempo Real** → **Proteção de Arquivos em Tempo Real** e clique no botão **Configurar**.
5. No bloco **Verificar as operações executadas nos contêineres do Windows**, defina as configurações da verificação de contêiners:

   - **Interromper o contêiner caso a desinfecção falhe**. O aplicativo pode não ter direitos de leitura e gravação suficientes para o objeto detectado. Nesse caso, não é possível desinfectar ou excluir o objeto detectado. Se essa caixa de seleção estiver marcada, o aplicativo bloqueia o objeto detectado e interrompe o contêiner. Se essa caixa de seleção estiver desmarcada, o aplicativo apenas bloqueia o objeto detectado.
   - **Não verificar as operações executadas nos contêineres do Windows**. Caso essa caixa de seleção esteja marcada, o aplicativo verificará o contêiner somente quando ele for iniciado. Se a caixa de seleção estiver desmarcada, o aplicativo verifica o contêiner continuamente em tempo real.
6. Salvar as novas configurações de segurança.

Como configurar a verificação de contêineres no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Proteção do Computador em Tempo Real** → **Proteção de Arquivos em Tempo Real**.
2. no painel de resultados do node **Proteção de Arquivos em Tempo Real**, clique no link **Propriedades**.

   A janela **Propriedades: Proteção de Arquivos em Tempo Real** é aberta.
3. No bloco **Verificar as operações executadas nos contêineres do Windows**, defina as configurações da verificação de contêiners:

   - **Interromper o contêiner caso a desinfecção falhe**. O aplicativo pode não ter direitos de leitura e gravação suficientes para o objeto detectado. Nesse caso, não é possível desinfectar ou excluir o objeto detectado. Se essa caixa de seleção estiver marcada, o aplicativo bloqueia o objeto detectado e interrompe o contêiner. Se essa caixa de seleção estiver desmarcada, o aplicativo apenas bloqueia o objeto detectado.
   - **Não verificar as operações executadas nos contêineres do Windows**. Caso essa caixa de seleção esteja marcada, o aplicativo verificará o contêiner somente quando ele for iniciado. Se a caixa de seleção estiver desmarcada, o aplicativo verifica o contêiner continuamente em tempo real.
4. Salvar alterações.

Uso da KSN

Para melhorar a proteção do computador, o Kaspersky Embedded Systems Security usa dados recebidos de usuários em todo o mundo. O Kaspersky Security Network foi criado para obter esses dados.

A funcionalidade KSN, pode não estar disponível no software nos EUA.

A Kaspersky Security Network (KSN) é uma infraestrutura de serviços em nuvem que permite o acesso à Base de Dados de Conhecimento on-line da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software. O uso dos dados do Kaspersky Security Network assegura rapidez nas respostas do Kaspersky Embedded Systems Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos. Se você faz parte da Kaspersky Security Network, os serviços KSN fornecem ao Kaspersky Embedded Systems Security informações sobre a categoria e a reputação dos arquivos verificados, bem como informações sobre a reputação dos endereços da Web verificados.

O uso da Kaspersky Security Network é voluntário. O aplicativo solicita que você use a KSN durante a configuração inicial do aplicativo. Os usuários podem iniciar ou descontinuar a participação na KSN a qualquer momento.

Para obter informação mais detalhada sobre o envio de informações estatísticas à Kaspersky, que são geradas durante a participação na KSN, e sobre o armazenamento e a destruição de tais informações, consulte a Declaração da Kaspersky Security Network e o site da Kaspersky. O arquivo ksn_<ID do idioma>.txt com o texto da Declaração da Kaspersky Security Network é incluído no kit de distribuição do aplicativo.

A infraestrutura dos bancos de dados de reputação da Kaspersky

O Kaspersky Embedded Systems Security é compatível com as seguintes soluções de infraestrutura para trabalhar com os bancos de dados de reputação Kaspersky:

- A *Kaspersky Security Network (KSN)* é a solução usada pela maioria dos aplicativos da Kaspersky. Os participantes da KSN recebem e enviam informações da Kaspersky sobre objetos detectados no computador do usuário para serem analisadas adicionalmente por seus analistas e para serem incluídas nos bancos de dados estatísticos e de reputação.

- A *Kaspersky Private Security Network (KPSN)* é uma solução que permite aos usuários de computadores que hospedam o Kaspersky Embedded Systems Security ou outros aplicativos da Kaspersky obtenham acesso aos bancos de dados de reputação da Kaspersky, além de outros dados estatísticos sem fazer o envio de dados para a Kaspersky a partir de seus próprios computadores. A KPSN foi desenvolvida para clientes corporativos que não podem participar da Kaspersky Security Network por qualquer um dos seguintes motivos:

  - Estações de trabalho locais não estão conectadas à Internet.

  - A transmissão de quaisquer dados para fora do país ou fora da rede local corporativa é proibida por lei ou restrita pelas políticas de segurança corporativa.

Ativação do uso da Kaspersky Security Network

Como ativar o uso da Kaspersky Security Network no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração da Kaspersky Security Network, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Esse procedimento abre uma janela; nessa janela, na lista de seções, selecione **Proteção do Computador em Tempo Real → Uso da KSN**.
4. Clique **Configurações**.
5. Use a caixa de seleção **Kaspersky Security Network** para ativar ou desativar o componente.

   Se você habilitou o uso da KSN, o Kaspersky Embedded Systems Security exibirá a Declaração da Kaspersky Security Network. Leia e aceite os termos de uso da Declaração da Kaspersky Security Network (KSN) caso concorde com eles.

   Por padrão, o Kaspersky Embedded Systems Security usa o modo Estendido da Kaspersky Security Network. O modo KSN estendido é um modo no qual o Kaspersky Embedded Systems Security envia dados adicionais para a Kaspersky.
6. Caso seja necessário, desmarque a caixa de seleção **Ativar modo KSN estendido**.
7. Salvar alterações.

Como resultado, se o uso da KSN estiver habilitado, o Kaspersky Embedded Systems Security usa informações sobre a reputação de arquivos, recursos da Web e aplicativos recebidos da Kaspersky Security Network.

Como ativar o uso da Kaspersky Security Network no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó secundário **Kaspersky Security Network**.
3. Na janela de propriedades da tarefa. Clique em **Propriedades**.
4. Use a caixa de seleção **Kaspersky Security Network** para ativar ou desativar o componente.

   Se você habilitou o uso da KSN, o Kaspersky Embedded Systems Security exibirá a Declaração da Kaspersky Security Network. Leia e aceite os termos de uso da Declaração da Kaspersky Security Network (KSN) caso concorde com eles.

   Por padrão, o Kaspersky Embedded Systems Security usa o modo Estendido da Kaspersky Security Network. O modo KSN estendido é um modo no qual o Kaspersky Embedded Systems Security envia dados adicionais para a Kaspersky.

5. Caso seja necessário, desmarque a caixa de seleção **Ativar modo KSN estendido**.

6. Salvar alterações.

Como resultado, se o uso da KSN estiver habilitado, o Kaspersky Embedded Systems Security usa informações sobre a reputação de arquivos, recursos da Web e aplicativos recebidos da Kaspersky Security Network.

Como ativar o uso da Kaspersky Security Network no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Vá para a seção **Proteção do Computador em Tempo Real** → **Uso da KSN** e clique no botão **Configurar**.

5. Na janela aberta, marque a caixa de seleção **Ativar a Kaspersky Security Network** para ativar o componente.

   Se você habilitou o uso da KSN, o Kaspersky Embedded Systems Security exibirá a Declaração da Kaspersky Security Network. Caso esteja de acordo, aceite os termos de uso da Kaspersky Security Network.

   Por padrão, o Kaspersky Embedded Systems Security usa o modo Estendido da Kaspersky Security Network. O modo KSN estendido é um modo no qual o Kaspersky Embedded Systems Security envia dados adicionais para a Kaspersky.

6. Caso seja necessário, desmarque a caixa de seleção **Ativar modo KSN estendido**.

7. Salvar alterações.

Assim, caso o uso da Kaspersky Security Network esteja ativado, o Kaspersky Embedded Systems Security usa informações sobre a reputação de arquivos, recursos da Web e aplicativos recebidos da Kaspersky Security Network.

Estatísticas de uso da Kaspersky Security Network

Enquanto a tarefa *Uso da KSN* estiver em execução, será possível visualizar as informações em tempo real sobre o número de objetos processados pelo Kaspersky Embedded Systems Security desde o momento em que a tarefa foi iniciada.

Para ver estatísticas de uso da KSN:

1. Na árvore do Console do Aplicativo, selecione o nó **Proteção do Computador em Tempo Real**.

2. Selecione o nó secundário **Kaspersky Security Network**.

   No painel de resultados, na seção **Estatísticas**, as estatísticas da tarefa são exibidas (consulte a tabela abaixo).

Estatísticas da KSN

Campo	Descrição
Solicitações de arquivo enviadas	Número de consultas de reputação de objeto enviadas pelo Kaspersky Embedded Systems Security para a KSN.
Arquivos não confiáveis na KSN	Número de objetos com reputação não confiável atribuídos pela KSN.
Erros de envio de solicitação	Número de solicitações da KSN processadas com um erro.
Estatísticas formadas	Número de pacotes estatísticos gerados e enviados à KSN.
Objetos removidos	Número de objetos excluídos com sucesso pelo Kaspersky Embedded Systems Security.
Objetos não removidos	Número de objetos que o Kaspersky Embedded Systems Security tentou excluir sem sucesso, devido, por exemplo, a um bloqueio no acesso ao objeto por parte de outro aplicativo.
Movidos para o Backup	Número de objetos copiados com sucesso no backup pelo Kaspersky Embedded Systems Security.
Objetos movidos para o backup	Número de objetos que o Kaspersky Embedded Systems Security não pôde copiar no backup devido a espaço insuficiente no disco, por exemplo. O aplicativo não desinfecta ou exclui arquivos que não podem ser movidos para o Backup.
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 envia apenas uma parte das solicitações de reputação do arquivo, de acordo com a recomendação dos especialistas da Kaspersky.

Os valores dos campos **Objetos removidos**, **Objetos não removidos**, **Movidos para o Backup**, **Objetos movidos para o backup** são gerados usando as estatísticas do componente Proteção de Arquivos em Tempo Real.

Limitações da Kaspersky Private Security Network

A *Kaspersky Private Security Network (KPSN)* é uma solução que permite aos usuários de computadores que hospedam o Kaspersky Embedded Systems Security ou outros aplicativos da Kaspersky obtenham acesso aos bancos de dados de reputação da Kaspersky, além de outros dados estatísticos sem fazer o envio de dados para a Kaspersky a partir de seus próprios computadores. A Kaspersky Private Security Network permite que o usuário use seu próprio banco de dados de reputação local para verificar a reputação de objetos (arquivos ou endereços da web). A reputação de um objeto adicionado ao banco de dados de reputação local tem uma prioridade mais alta do que uma adicionada à KSN/KPSN. Por exemplo, imagine que o Kaspersky Embedded Systems Security está verificando um computador e solicita a reputação de um arquivo na KSN/KPSN. Se o arquivo tiver uma reputação *Não confiáveis* no banco de dados de reputação local, mas tiver uma reputação *Confiáveis* na KSN/KPSN, o Kaspersky Embedded Systems Security detectará o arquivo como *Não confiáveis* e executará a ação definida para ameaças detectadas.

No entanto, em alguns casos, o Kaspersky Embedded Systems Security pode não solicitar a reputação de um objeto na KSN/KPSN. Se for esse o caso, o Kaspersky Embedded Systems Security não receberá dados do banco de dados de reputação local da KPSN. O Kaspersky Embedded Systems Security pode não solicitar a reputação de um objeto na KSN/KPSN pelos seguintes motivos:

- Os aplicativos Kaspersky estão usando bancos de dados de reputação offline. Os bancos de dados de reputação offline são projetados para otimizar recursos durante a operação dos aplicativos Kaspersky e para proteger objetos extremamente importantes no computador. Os bancos de dados de reputação offline são criados por especialistas da Kaspersky com base nos dados da Kaspersky Security Network. Os aplicativos Kaspersky atualizam os bancos de dados de reputação offline com bancos de dados de antivírus do aplicativo específico. Se os bancos de dados de reputação offline contiverem informações sobre um objeto que está sendo verificado, o aplicativo não solicita a reputação desse objeto de KSN/KPSN.

- As exclusões de verificação (zona confiável) são definidas nas configurações do aplicativo. Nesse caso, o aplicativo não leva em consideração a reputação do objeto no banco de dados de reputação local.

- O aplicativo usa as tecnologias de otimização da verificação, como iSwift ou iChecker, ou está armazenando em cache as solicitações de reputação para a KSN /KPSN. Nesse caso, o aplicativo pode não solicitar a reputação de objetos verificados anteriormente.

- Para otimizar sua carga de trabalho, o aplicativo verifica arquivos de um determinado formato e tamanho. A lista de formatos e limites de tamanho relevantes é determinada pelos especialistas da Kaspersky. Esta lista é atualizada com os bancos de dados de antivírus do aplicativo.

Configurações de proxy da KSN

Computadores de usuários gerenciados pelo Servidor de Administração do Kaspersky Security Center podem interagir com a KSN por meio do serviço de Proxy da KSN.

O serviço de Proxy da KSN fornece os seguintes recursos:

- O computador do usuário pode consultar a KSN e envia informações para a KSN, mesmo sem estar com acesso direito à Internet.

- O serviço de KSN Proxy armazena em cache os dados processados, reduzindo assim a carga no canal de comunicação da rede externa e acelerando recebimento de informações solicitadas pelo computador do usuário.

Por padrão, depois que a KSN for habilitada e a Declaração KSN for aceita, o aplicativo usará um servidor proxy para se conectar à Kaspersky Security Network. O servidor proxy usado pelo aplicativo é o Servidor de Administração do Kaspersky Security Center via porta TCP 13111. Assim, caso o KSN Proxy esteja indisponível, será necessário verificar a operação do dispositivo como um servidor proxy da KSN. É necessário verificar os seguintes aspectos:

- O serviço *ksnproxy* está sendo executado no Servidor de Administração.

- O Firewall no computador não está bloqueando a porta 13111.

É possível configurar o uso do Proxy da KSN da seguinte forma: habilite ou desabilite o Proxy da KSN e configure a porta para a conexão. Para fazer isso, é preciso abrir as propriedades do Servidor de Administração. Para obter mais informações sobre a configuração do Proxy da KSN, consulte a ajuda do Kaspersky Security Center. Também é possível habilitar ou desabilitar o Proxy da KSN para computadores individuais na política do Kaspersky Embedded Systems Security.

Como ativar o KSN Proxy no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Esse procedimento abre uma janela; nessa janela, na lista de seções, selecione **Proteção do Computador em Tempo Real → Uso da KSN**.
4. Clique **Configurações**.
5. No bloco **Configurações do proxy da KSN**, use a caixa de seleção **Usar o Servidor de Administração como um servidor proxy da KSN** para ativar ou desativar o Proxy da KSN.
6. Caso seja necessário, marque a caixa de seleção **Usar servidores da Kaspersky Security Network se o servidor proxy da KSN não estiver disponível**.

   Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security usará os servidores da KSN quando o serviço Proxy da KSN estiver indisponível. Os servidores da KSN podem ser localizados no lado da Kaspersky e no lado de terceiros (quando a Kaspersky Private Security Network for usada).
7. Salvar alterações.

Como ativar o KSN Proxy no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó secundário **Kaspersky Security Network**.
3. Na janela de propriedades da tarefa. Clique em **Propriedades**.
4. No bloco **Configurações do proxy da KSN**, use a caixa de seleção **Usar o Servidor de Administração como um servidor proxy da KSN** para ativar ou desativar o Proxy da KSN.
5. Caso seja necessário, marque a caixa de seleção **Usar servidores da Kaspersky Security Network se o servidor proxy da KSN não estiver disponível**.

   Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security usará os servidores da KSN quando o serviço Proxy da KSN estiver indisponível. Os servidores da KSN podem ser localizados no lado da Kaspersky e no lado de terceiros (quando a Kaspersky Private Security Network for usada).
6. Salvar alterações.

Como ativar o KSN Proxy no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos) → Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção do Computador em Tempo Real** → **Uso da KSN** e clique no botão **Configurar**.
5. Marque ou desmarque a caixa de seleção **Usar o Servidor de Administração como um servidor proxy da KSN** para ativar ou desativar o proxy da KSN.
6. Caso seja necessário, marque a caixa de seleção **Usar servidores da Kaspersky Security Network se o servidor proxy da KSN não estiver disponível**.

   Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security usará os servidores da KSN quando o serviço Proxy da KSN estiver indisponível. Os servidores da KSN podem ser localizados no lado da Kaspersky e no lado de terceiros (quando a Kaspersky Private Security Network for usada).
7. Salvar alterações.

O endereço do Proxy da KSN corresponde ao endereço do Servidor de Administração. Quando o nome de domínio do Servidor de Administração é alterado, é preciso atualizar manualmente o endereço do Proxy da KSN.

Prevenção de Exploit

O Kaspersky Embedded Systems Security oferece a capacidade de proteger a memória do processo contra exploits. Essa funcionalidade é implementada pelo componente Prevenção de Exploits que pode ser usado para alterar o status de atividade do componente e configurar a proteção de processos contra exploits.

O componente de Prevenção de exploit detecta o código do programa que aproveita as vulnerabilidades do computador para tirar proveito dos privilégios de administrador ou para realizar atividades mal-intencionadas. Por exemplo, exploits podem usar um ataque de estouro de buffer. Para fazer isso, o exploit envia uma grande quantidade de dados para um aplicativo vulnerável. Ao processar esses dados, o aplicativo vulnerável executa códigos maliciosos. Como resultado desse ataque, o exploit pode iniciar uma instalação não autorizada de malwares. Quando há uma tentativa de executar um arquivo executável de um aplicativo vulnerável que não foi realizada pelo usuário, o Kaspersky Embedded Systems Security bloqueia a execução do arquivo ou notifica o usuário. 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 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 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.

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:

- **Bloquear**. Se este modo for selecionado, o Kaspersky Embedded Systems Security encerrará um processo protegido após a detecção de uma tentativa de exploit se uma técnica de redução de impacto ativa tiver sido aplicada ao processo.

  Após detecção de uma tentativa de exploração de uma vulnerabilidade em um processo crítico do sistema operacional protegido, o Kaspersky Embedded Systems Security encerrará o processo, independentemente do modo indicado nas configurações do componente de Prevenção de Exploits.

- **Informar** (durante o funcionamento no Kaspersky Security Center Web Console – **Informar**). Aplique esse modo para receber informações sobre exemplos de exploits em processos protegidos usando eventos no log de segurança. O processo violado continua a ser executado.

  Se esse modo for selecionado, o Kaspersky Embedded Systems Security cria eventos para registrar em log todas as tentativas de explorar vulnerabilidades. Selecionado por padrão.

Ativar e desativar a Prevenção de Exploit

O Kaspersky Embedded Systems Security permite monitorar os arquivos executáveis que estão sendo executados por aplicativos vulneráveis. Se o Kaspersky Embedded Systems Security detectar que um arquivo executável de um aplicativo vulnerável foi executado por outra coisa além do usuário, o Kaspersky Embedded Systems Security executará a ação selecionada (por exemplo, bloqueará a operação).

Como ativar ou desativar a Prevenção de Exploits no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Esse procedimento abre uma janela; nessa janela, na lista de seções, selecione **Proteção do Computador em Tempo Real → Prevenção de Exploits**.
4. Clique **Configurações**.
5. Use a caixa de seleção **Prevenção de Exploits** para ativar ou desativar o componente.
6. Na guia **Geral**, selecione um modo de prevenção de exploits: **Bloquear** ou **Informar**.
7. Caso seja necessário, desmarque a caixa de seleção **Prevenção de Exploits** para desativar o componente.
8. Salvar alterações.

Como ativar ou desativar a Prevenção de Exploits no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó secundário **Prevenção de Exploits**.
3. Na janela de propriedades da tarefa. Clique em **Propriedades**.
4. Use a caixa de seleção **Prevenção de Exploits** para ativar ou desativar o componente.
5. Na guia **Geral**, selecione um modo de prevenção de exploits: **Bloquear** ou **Informar**.
6. Caso seja necessário, desmarque a caixa de seleção **Prevenção de Exploits** para desativar o componente.
7. Salvar alterações.

Como ativar ou desativar a Prevenção de Exploits no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção do Computador em Tempo Real** → **Prevenção de Exploits** e clique no botão **Configurar**.
5. Esse procedimento abre uma janela; nessa janela, em **Modo de Prevenção de Exploits**, marque a caixa de seleção **Prevenir exploits de processos vulneráveis** para ativar o componente.
6. Selecione um modo de Prevenção de Exploits: **Bloquear** ou **Informar**.
7. Caso seja necessário, desmarque a caixa de seleção **Prevenir exploits de processos vulneráveis** para desativar o componente.
8. Salvar alterações.

Ativar e desativar a proteção da memória

O Kaspersky Embedded Systems Security bloqueia processos externos que tentam obter acesso aos processos do sistema. Por padrão, a proteção da memória de processos do sistema está ativada.

Como ativar ou desativar a proteção de memória no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Esse procedimento abre uma janela; nessa janela, na lista de seções, selecione **Proteção do Computador em Tempo Real** → **Prevenção de Exploits**.
4. Clique **Configurações**.
5. No bloco **Geral**, marque a caixa de seleção **Ativar a proteção da memória de processos do sistema**.
6. Caso seja necessário, desmarque a caixa de seleção **Ativar a proteção da memória de processos do sistema**.
7. Salvar alterações.

Como ativar ou desativar a proteção de memória no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó secundário **Prevenção de Exploits**.
3. Na janela de propriedades da tarefa. Clique em **Propriedades**.
4. No bloco **Geral**, marque a caixa de seleção **Ativar a proteção da memória de processos do sistema**.
5. Caso seja necessário, desmarque a caixa de seleção **Ativar a proteção da memória de processos do sistema**.
6. Salvar alterações.

Como ativar ou desativar a proteção de memória no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção do Computador em Tempo Real** → **Prevenção de Exploits** e clique no botão **Configurar**.
5. Na janela que é aberta, no bloco **Proteção da memória de processos do sistema**, marque a caixa de seleção **Proteção da memória de processos do sistema**.

6. Caso seja necessário, desmarque a caixa de seleção **Proteção da memória de processos do sistema** para desativar a proteção da memória do processo do sistema.

7. Salvar alterações.

Criar uma lista de processos confiáveis.

Por padrão, o componente Prevenção de Exploits protege vários processos. O aplicativo pode gerar automaticamente a lista de processos protegidos. Também é possível adicionar ou remover manualmente os processos.

Como gerenciar a lista de processos protegidos no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Esse procedimento abre uma janela; nessa janela, na lista de seções, selecione **Proteção do Computador em Tempo Real → Prevenção de Exploits**.

4. Clique **Configurações**.

5. Na guia **Processos protegidos**, selecione uma das seguintes opções para proteger os processos contra a invasão de código malicioso:

   - **Detectar processos protegidos automaticamente**. Caso essa opção seja selecionada, o aplicativo criará automaticamente uma lista de processos protegidos.

   - **Proteger apenas os processos da lista abaixo**. Caso essa opção seja selecionada, será possível selecionar os processos que deseja proteger.

6. Caso selecione **Proteger apenas os processos da lista abaixo**, será possível editar a lista de processos protegidos por meio de uma das seguintes ações:

   - Caso seja necessário, clique em **Adicionar** e selecione um processo que deseja adicionar à lista de processos protegidos.

   - Caso queira excluir um processo da lista de processos protegidos criada, selecione o processo na lista e clique em **Excluir**.

     O botão **Excluir** ficará disponível depois que um ou mais processos na lista for selecionado.

7. Salvar alterações.

Como gerenciar a lista de processos protegidos com o uso do Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.

2. Selecione o nó secundário **Prevenção de Exploits**.

3. Na janela de propriedades da tarefa. Clique em **Propriedades**.

4. Na guia **Processos protegidos**, selecione uma das seguintes opções para proteger os processos contra a invasão de código malicioso:

   - **Detectar processos protegidos automaticamente**. Caso essa opção seja selecionada, o aplicativo criará automaticamente uma lista de processos protegidos.

   - **Proteger apenas os processos da lista abaixo**. Caso essa opção seja selecionada, será possível selecionar os processos que deseja proteger.

5. Caso selecione **Proteger apenas os processos da lista abaixo**, será possível editar a lista de processos protegidos por meio de uma das seguintes ações:

   - Caso seja necessário, clique em **Adicionar** e selecione um processo que deseja adicionar à lista de processos protegidos.

   - Caso queira excluir um processo da lista de processos protegidos criada, selecione o processo na lista e clique em **Excluir**.

     O botão **Excluir** ficará disponível depois que um ou mais processos na lista for selecionado.

6. Salvar alterações.

Como gerenciar a lista de processos protegidos no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Vá para a seção **Proteção do Computador em Tempo Real** → **Prevenção de Exploits** e clique no botão **Configurar**.

5. Em **Lista de processos protegidos**, selecione uma das seguintes opções para proteger os processos contra invasão de código malicioso:

   - **Detectar processos protegidos automaticamente**. Caso essa opção seja selecionada, o aplicativo criará automaticamente uma lista de processos protegidos.

   - **Proteger apenas os processos da lista abaixo**. Caso essa opção seja selecionada, será possível adicionar, editar e remover os processos que deseja proteger.

6. Caso tenha selecionado **Proteger apenas os processos da lista abaixo**, escolha uma das seguintes opções:

   - Clique em **Adicionar** para abrir a janela **Processo protegido** e, em seguida, nessa janela:

     a. Marque a caixa de seleção **Processo protegido**.

     b. No campo **Nome do processo**, insira o nome do processo.

     c. Salvar alterações.

   - Caso seja necessário, edite as configurações do processo na lista de processos protegidos. Para isso, execute as seguintes ações:

     a. Selecione um processo na lista de processos protegidos.

     b. Clique **Editar**. O botão **Editar** ficará disponível depois que um ou mais processos na lista for selecionado.

     c. Na janela **Processo protegido**, marque ou desmarque a caixa de seleção **Processo protegido**.

     d. Caso seja necessário, edite o nome do processo no campo **Nome do processo**.

     e. Salvar alterações.

   - Caso seja necessário, é possível remover um processo da lista de processos protegidos. Para isso, execute as seguintes ações:

     a. Selecione um ou mais processos na lista de processos protegidos.

     b. Clique **Excluir**. O botão **Excluir** ficará disponível depois que um ou mais processos na lista for selecionado.

7. Salvar alterações.

Mecanismo de Remediação

O Mecanismo de Remediação permite que o Kaspersky Embedded Systems Security desfaça ações executadas por Malwares no sistema operacional.

Ao reverter a atividade de malware no sistema operacional, o Kaspersky Embedded Systems Security executa as seguintes ações:

- **Atividade de arquivo**
  - Exclui arquivos executáveis que foram criados pelo malware em todas as mídias, exceto unidades de rede.
  - Exclui arquivos executáveis que foram criados por programas infiltrados por malware.
  - Restaura arquivos que foram modificados ou excluídos pelo malware.

  O recurso de recuperação de arquivo tem **algumas limitações**.

  - O aplicativo somente restaura arquivos em dispositivos que tenham o sistema de arquivos NTFS ou FAT32.
  - O aplicativo pode restaurar arquivos com as seguintes extensões: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
  - Não é possível restaurar arquivos localizados em unidades de rede ou em CDs/DVDs regraváveis.
  - Não é possível restaurar arquivos que foram criptografados com Encryption File System (EFS). Para obter mais detalhes sobre a operação do EFS, visite o site da Microsoft.
  - O aplicativo não monitora as modificações dos arquivos feitas por processos no nível do kernel do sistema operacional.
  - O aplicativo não monitora as modificações feitas nos arquivos por meio de uma interface de rede (por exemplo, se um arquivo estiver armazenado em uma pasta compartilhada e um processo for iniciado remotamente em outro computador).

- **Atividade de registro**
  - Exclui chaves do registro que foram criadas pelo malware.

  O Kaspersky Embedded Systems Security não restaura as chaves do registro modificadas ou excluídas pelo malware.

- **Atividade de sistema**
  - Encerra processos que foram iniciados pelo malware.
  - Encerra processos invadidos por aplicativos maliciosos.

O Kaspersky Embedded Systems Security não reinicia os processos pausados pelo malware.

- **Atividade de rede**
  - Bloqueia a atividade de rede do malware.
  - Bloqueia a atividade de rede de processos que foram invadidos pelo malware.

A reversão das ações de um aplicativo malicioso pode ser iniciada pelo componente Proteção de Arquivos em Tempo Real ou durante uma verificação por demanda.

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

Como ativar ou desativar o componente Mecanismo de Remediação no Console de Administração do Kaspersky Security Center

1. Abra as configurações do componente Mecanismo de Remediação na política que deseja configurar.
   a. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados**.
   b. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
   c. Selecione a guia **Políticas**.
   d. Abra a janela de propriedades da política com um clique duplo no nome da política.
   e. Na janela de propriedades da política, acesse a seção **Proteção do Computador em Tempo Real**.
   f. No bloco **Mecanismo de Remediação**, clique no botão **Configurações**.
   A janela **Mecanismo de Remediação** é exibida na guia **Geral**.
2. Execute uma das seguintes ações:
   - Marque a caixa de seleção **Mecanismo de Remediação** caso queira ativar o componente do Mecanismo de Remediação.
   - Desmarque a caixa de seleção **Mecanismo de Remediação** caso queira desativar o componente do Mecanismo de Remediação.
3. Clique no botão **OK** na subseção **Mecanismo de Remediação**.
4. Clique no botão **OK** na janela **Propriedades: <Nome da política>**.

Como ativar ou desativar o componente do Mecanismo de Remediação no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, selecione o node **Proteção do Computador em Tempo Real** → **Mecanismo de Remediação**.
2. Clique no link **Propriedades** no painel de resultados.

   A janela **Mecanismo de Remediação** é exibida na guia **Geral**.
3. Execute uma das seguintes ações:
   - Marque a caixa de seleção **Mecanismo de Remediação** caso queira ativar o componente do Mecanismo de Remediação.
   - Desmarque a caixa de seleção **Mecanismo de Remediação** caso queira desativar o componente do Mecanismo de Remediação.
4. Clique no botão **OK** na subseção **Mecanismo de Remediação**.

Como ativar ou desativar o componente Mecanismo de Remediação no Kaspersky Security Center Web Console

1. Abra as configurações do componente Mecanismo de Remediação na política que deseja configurar.
   a. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
   b. Clique no nome da política do Kaspersky Embedded Systems Security.

      A janela de propriedades da política é exibida.
   c. Selecione a guia **Configurações do aplicativo**.
   d. Selecione a seção **Proteção do Computador em Tempo Real**.
   e. No bloco **Mecanismo de Remediação**, clique no botão **Configurar**.

      A janela **Mecanismo de Remediação** é aberta.
2. Execute uma das seguintes ações:
   - Marque a caixa de seleção **Mecanismo de Remediação** caso queira ativar o componente do Mecanismo de Remediação.
   - Desmarque a caixa de seleção **Mecanismo de Remediação** caso queira desativar o componente do Mecanismo de Remediação.
3. Clique no botão **OK** na subseção **Mecanismo de Remediação**.
4. Na janela **<Nome da política>**, clique em **Salvar**.

Detecção de Comportamento

O componente Detecção de Comportamento recebe dados sobre as ações dos aplicativos em seu computador e fornece essas informações a outros componentes de proteção para melhorar o desempenho. O componente Detecção de Comportamento utiliza Assinaturas de Fluxos de Comportamentos (BSS, Behavior Stream Signatures) para aplicativos. Se a atividade de um aplicativo corresponder a um padrão de atividades perigosas, o Kaspersky Embedded Systems Security executará a ação de resposta selecionada. A funcionalidade do Kaspersky Embedded Systems Security com base em padrões de atividades perigosas fornece Defesa Proativa ao computador.

Ativação e desativação da proteção por criptografia para pastas locais

Como ativar ou desativar o componente de Detecção de Comportamento no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção do Computador em Tempo Real**.
4. Na seção **Detecção de Comportamento**, clique em **Configurações**.
5. Marque ou desmarque a caixa de seleção **Detecção de Comportamento** para ativar ou desativar o componente.
6. Vá para a guia **Geral**.
7. Use a caixa de seleção **Ativar a proteção de pastas locais contra criptografia externa** para ativar ou desativar a opção. Se essa caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security responde a atividades maliciosas com a ação especificada abaixo.
8. Selecione a ação relevante na seção **Ação ao detectar atividade de malware**:
   - **Excluir**. Se este item for selecionado, ao detectar uma atividade maliciosa, o Kaspersky Embedded Systems Security excluirá o arquivo executável do aplicativo malicioso e criará uma cópia do arquivo no Backup.
   - **Bloquear**. Se este item for selecionado, ao detectar atividade maliciosa, o Kaspersky Embedded Systems Security encerrará este aplicativo.
   - **Informar**. Se este item for selecionado e a atividade de malware de um aplicativo for detectada, o Kaspersky Embedded Systems Security adiciona informações sobre a atividade de malware do aplicativo à lista de ameaças ativas.
9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como ativar ou desativar o componente de Detecção de Comportamento no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção do Computador em Tempo Real** → **Detecção de Comportamento** e clique no botão **Configurar**.

   A janela **Detecção de Comportamento** é aberta.
5. Use a caixa de seleção **Ativar Detecção de Comportamento** para ativar ou desativar o componente.
6. Vá para a guia **Geral**.
7. Use a caixa de seleção **Ativar a proteção de pastas locais contra criptografia externa** para ativar ou desativar a opção. Se essa caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security responde a atividades maliciosas com a ação especificada abaixo.
8. Selecione a ação relevante na seção **Na detecção de criptografia externa de pastas compartilhadas**:
   - **Excluir**. Se este item for selecionado, ao detectar uma atividade maliciosa, o Kaspersky Embedded Systems Security excluirá o arquivo executável do aplicativo malicioso e criará uma cópia do arquivo no Backup.
   - **Bloquear**. Se este item for selecionado, ao detectar atividade maliciosa, o Kaspersky Embedded Systems Security encerrará este aplicativo.
   - **Informar**. Se este item for selecionado e a atividade de malware de um aplicativo for detectada, o Kaspersky Embedded Systems Security adiciona informações sobre a atividade de malware do aplicativo à lista de ameaças ativas.
9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como ativar ou desativar o componente de Detecção de Comportamento no Console do Aplicativo

1. Na árvore do Kaspersky Embedded Systems Security Console, selecione **Proteção do Computador em Tempo Real** → **Detecção de Comportamento**.
2. No painel de resultados do nó **Detecção de Comportamento**, clique em **Propriedades**.

   Esse procedimento abre a janela **Propriedades: Detecção de Comportamento**.
3. Marque a caixa de seleção **Objetos a serem detectados**.
4. Vá para a guia **Geral**.

5. Use a caixa de seleção **Ativar a proteção de pastas locais contra criptografia externa** para ativar ou desativar a opção. Se essa caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security responde a atividades maliciosas com a ação especificada abaixo.

6. Selecione a ação relevante na seção **Na detecção de criptografia externa de pastas compartilhadas**:

   - **Excluir**. Se este item for selecionado, ao detectar uma atividade maliciosa, o Kaspersky Embedded Systems Security excluirá o arquivo executável do aplicativo malicioso e criará uma cópia do arquivo no Backup.

   - **Bloquear**. Se este item for selecionado, ao detectar atividade maliciosa, o Kaspersky Embedded Systems Security encerrará este aplicativo.

   - **Informar**. Se este item for selecionado e a atividade de malware de um aplicativo for detectada, o Kaspersky Embedded Systems Security adiciona informações sobre a atividade de malware do aplicativo à lista de ameaças ativas.

7. Salvar alterações.

Proteção de pastas compartilhadas contra criptografia externa

O componente só monitora operações executadas com arquivos armazenados em dispositivos de armazenamento em massa com o sistema de arquivos NTFS e que não sejam criptografados com EFS.

A proteção de pastas compartilhadas contra criptografia externa fornece a análise da atividade em pastas compartilhadas. Se esta atividade combinar com uma assinatura de fluxo de comportamento que é típica para a criptografia externa, o Kaspersky Embedded Systems Security executa a ação selecionada.

Caso uma tentativa de modificar arquivos em pastas compartilhadas seja detectada, o Kaspersky Embedded Systems Security executará as seguintes ações:

- Bloqueia o acesso à modificação de arquivos para a sessão que iniciou a atividade maliciosa (o arquivo ficará disponível somente para leitura).

- Cria cópias de backup dos arquivos que estão sendo modificados.

- Adiciona uma entrada nos relatórios da interface do aplicativo local e envia informações sobre atividades maliciosas detectadas ao Kaspersky Security Center.

- Além disso, se o componente Mecanismo de remediação for ativado, os arquivos modificados serão restaurados a partir de cópias de backup.

Ativar e desativar a proteção de pastas compartilhadas contra criptografia externa

Por padrão, a proteção de pastas compartilhadas contra criptografia externa está ativada e funcionando no modo recomendado pelos especialistas da Kaspersky. Para configurar essa funcionalidade, é possível criar um escopo de proteção e, caso seja necessário, configurar exclusões. Por padrão, o aplicativo identifica automaticamente as pastas compartilhadas e monitora a atividade de arquivos em todas as pastas. Caso uma tentativa de criptografar arquivos externos em pastas compartilhadas seja detectada, o Kaspersky Embedded Systems Security bloqueará a sessão do usuário remoto por uma hora (por padrão).

Depois que o Kaspersky Embedded Systems Security é instalado, a proteção de pastas compartilhadas contra criptografia externa será limitada até que o computador seja reiniciado.

Como ativar ou desativar a proteção de pastas compartilhadas contra criptografia externa no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção do Computador em Tempo Real**.
4. Na seção **Detecção de Comportamento**, clique em **Configurações**.
5. Marque ou desmarque a caixa de seleção **Detecção de Comportamento** para ativar ou desativar o componente.
6. Vá para a guia **Proteção de pastas compartilhadas**.
7. Use a caixa de seleção **Proteger pastas compartilhadas** para ativar ou desativar a opção.
8. Selecione a ação relevante na seção **Proteção de pastas compartilhadas contra criptografia externa**:
   - **Bloquear conexão por N min**. Caso esta opção seja selecionada, ao detectar uma tentativa de modificação dos arquivos em pastas compartilhadas, o Kaspersky Embedded Systems Security bloqueia o acesso à modificação de arquivo (somente leitura) para a sessão que iniciou a atividade maliciosa e cria cópias de backup dos arquivos modificados.

     Caso o componente Mecanismo de Remediação seja ativado e a opção **Bloquear conexão por N min** seja selecionada, os arquivos modificados são restaurados a partir das cópias de backup.

   - **Informar**. Caso essa opção seja selecionada, se uma tentativa de modificação de arquivos em pastas compartilhadas for detectada, o Kaspersky Embedded Systems Security adicionará informações sobre essa tentativa de modificação de arquivos em pastas compartilhadas na lista de ameaças ativas, adicionará um registro aos relatórios da interface local do aplicativo e enviará informações sobre a detecção de atividades maliciosas para o Kaspersky Security Center.

9. Se necessário, edite um escopo de proteção e defina exclusões.
10. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como ativar ou desativar a proteção de pastas compartilhadas contra criptografia externa no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção do Computador em Tempo Real** → **Detecção de Comportamento** e clique no botão **Configurar**.

   A janela **Detecção de Comportamento** é aberta.
5. Use a caixa de seleção **Ativar Detecção de Comportamento** para ativar ou desativar o componente.
6. Vá para a guia **Proteção de pastas compartilhadas**.
7. Use a caixa de seleção **Ativar a proteção de pastas compartilhadas contra criptografia externa** para ativar ou desativar a opção.
8. Selecione a ação relevante na seção **Detecção de criptografia externa**:

   - **Bloquear conexão**. Se essa opção for selecionada, ao detectar uma tentativa de modificar arquivos em pastas compartilhadas, o Kaspersky Embedded Systems Security bloqueia o acesso à modificação de arquivos (somente leitura) para a sessão que iniciou a atividade maliciosa e cria cópias de backup dos arquivos modificados.

     Se o componente Mecanismo de Remediação estiver ativado e a opção **Bloquear conexão** estiver selecionada, os arquivos modificados são restaurados a partir das cópias de backup.

   - **Informar**. Caso essa opção seja selecionada, se uma tentativa de modificação de arquivos em pastas compartilhadas for detectada, o Kaspersky Embedded Systems Security adicionará informações sobre essa tentativa de modificação de arquivos em pastas compartilhadas na lista de ameaças ativas, adicionará um registro aos relatórios da interface local do aplicativo e enviará informações sobre a detecção de atividades maliciosas para o Kaspersky Security Center.
9. Se necessário, edite um escopo de proteção e defina exclusões.
10. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como ativar ou desativar a proteção de pastas compartilhadas contra criptografia externa no Console do Aplicativo

1. Na árvore do Kaspersky Embedded Systems Security Console, selecione **Proteção do Computador em Tempo Real → Detecção de Comportamento**.
2. No painel de resultados do nó **Detecção de Comportamento**, clique em **Propriedades**.

   Esse procedimento abre a janela **Propriedades: Detecção de Comportamento**.
3. Marque a caixa de seleção **Objetos a serem detectados**.
4. Vá para a guia **Proteção de pastas compartilhadas**.
5. Use a caixa de seleção **Proteger pastas compartilhadas** para ativar ou desativar a opção.
6. Selecione a ação relevante na seção **Proteção de pastas compartilhadas contra criptografia externa**:
   - **Bloquear conexão por N min**. Caso esta opção seja selecionada, ao detectar uma tentativa de modificação dos arquivos em pastas compartilhadas, o Kaspersky Embedded Systems Security bloqueia o acesso à modificação de arquivo (somente leitura) para a sessão que iniciou a atividade maliciosa e cria cópias de backup dos arquivos modificados.

     Caso o componente Mecanismo de Remediação seja ativado e a opção **Bloquear conexão por N min** seja selecionada, os arquivos modificados são restaurados a partir das cópias de backup.
   - **Informar**. Caso essa opção seja selecionada, se uma tentativa de modificação de arquivos em pastas compartilhadas for detectada, o Kaspersky Embedded Systems Security adicionará informações sobre essa tentativa de modificação de arquivos em pastas compartilhadas na lista de ameaças ativas, adicionará um registro aos relatórios da interface local do aplicativo e enviará informações sobre a detecção de atividades maliciosas para o Kaspersky Security Center.
7. Se necessário, edite um escopo de proteção e defina exclusões.
8. Salvar alterações.

Criação do escopo da proteção

Um *escopo de proteção* é uma lista de caminhos para pastas compartilhadas nas quais o Kaspersky Embedded Systems Security monitora a atividade do arquivo. O Kaspersky Embedded Systems Security tem suporte a variáveis de ambiente e aos caracteres `*` e `?` na inserção de uma máscara: por padrão, o aplicativo identifica automaticamente as pastas compartilhadas e rastreia a atividade de arquivos em todas as pastas.

Excluir uma pasta do escopo de proteção pode reduzir a quantidade de falsos positivos se a sua organização usar criptografia de dados ao trocar arquivos usando pastas compartilhadas. Por exemplo, o componente Detecção de Comportamento pode gerar falsos positivos quando o usuário trabalhar com arquivos com a extensão ENC em uma pasta compartilhada. Essa atividade corresponde a um padrão comportamental típico da criptografia externa. Se houver dados criptografados em uma pasta compartilhada, adicione essa pasta às exclusões.

Também é possível excluir computadores se quiser que as tentativas de criptografia externa provenientes desses computadores sejam ignoradas.

Como configurar o escopo de proteção no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção do Computador em Tempo Real**.
4. Na seção **Detecção de Comportamento**, clique em **Configurações**.
5. Marque ou desmarque a caixa de seleção **Detecção de Comportamento** para ativar ou desativar o componente.
6. Vá para a guia **Proteção de pastas compartilhadas**.
7. No bloco **Escopo de proteção**, clique no botão **Configurar**.
8. Na janela que é aberta, selecione o modo **Somente pastas especificadas compartilhadas**.
9. Clique **Adicionar**.
10. Isso abre uma janela; nessa janela, insira o caminho para a pasta compartilhada que deseja incluir no escopo de proteção (por exemplo, `C:\Share`).

    Para adicionar uma pasta compartilhada ao escopo de proteção, use um caminho local.

11. Clique **OK**.
12. Caso seja necessário, configure as exclusões do escopo de proteção:
    a. No bloco **Exclusões**, clique no botão **Configurar**.
    b. Clique no botão **Adicionar** na janela que se abre.
    c. Na janela exibida, insira o caminho para a pasta ou arquivo.

Usar máscaras:

- O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas.

- Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

- O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/`(delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.

É possível excluir um objeto da verificação sem excluí-lo da lista de objetos no escopo de proteção. Para fazer isso, desmarque a caixa de seleção ao lado do objeto.

13. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como configurar o escopo de proteção no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção do Computador em Tempo Real** → **Detecção de Comportamento** e clique no botão **Configurar**.

   A janela **Detecção de Comportamento** é aberta.
5. Use a caixa de seleção **Ativar Detecção de Comportamento** para ativar ou desativar o componente.
6. Vá para a guia **Proteção de pastas compartilhadas**.
7. Em **Escopo de proteção**, selecione o modo **Somente pastas compartilhadas especificadas**.
8. Clique **Adicionar**.
9. Isso abre uma janela; nessa janela, insira o caminho para a pasta compartilhada que deseja incluir no escopo de proteção (por exemplo, `C:\Share`).

   Para adicionar uma pasta compartilhada ao escopo de proteção, use um caminho local.
10. Clique **OK**.

11. Caso seja necessário, configure as exclusões do escopo de proteção:

    a. No bloco **Objeto a ser excluído**, clique no botão **Adicionar**.

    b. Na janela exibida, insira o caminho para a pasta ou arquivo.

    Usar máscaras:

    - O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas.

    - Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

    - O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/`(delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.

    É possível excluir um objeto da verificação sem excluí-lo da lista de objetos no escopo de proteção. Para fazer isso, desmarque a caixa de seleção ao lado do objeto.

12. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como configurar o escopo de proteção no Console do Aplicativo

1. Na janela da política, selecione **Proteção do Computador em Tempo Real**.
2. Na seção **Detecção de Comportamento**, clique em **Configurações**.
3. Na árvore do Kaspersky Embedded Systems Security Console, selecione **Proteção do Computador em Tempo Real** → **Detecção de Comportamento**.
4. No painel de resultados do nó **Detecção de Comportamento**, clique em **Propriedades**.

   Esse procedimento abre a janela **Propriedades: Detecção de Comportamento**.
5. Marque ou desmarque a caixa de seleção **Detecção de Comportamento** para ativar ou desativar o componente.
6. Vá para a guia **Proteção de pastas compartilhadas**.
7. No bloco **Escopo de proteção**, clique no botão **Configurar**.
8. Na janela que é aberta, selecione o modo **Somente pastas especificadas compartilhadas**.
9. No bloco **Escopo de proteção**, clique no botão **Adicionar**.

10. Isso abre uma janela; nessa janela, insira o caminho para a pasta compartilhada que deseja incluir no escopo de proteção (por exemplo, `C:\Share`).

    Para adicionar uma pasta compartilhada ao escopo de proteção, use um caminho local.

11. Clique **OK**.

12. Caso seja necessário, configure as exclusões do escopo de proteção:

    a. No bloco **Exclusões**, clique no botão **Configurações**.

    b. No bloco **Exclusões por máscara**, clique no botão **Adicionar**.

    c. Na janela exibida, insira o caminho para a pasta ou arquivo.

    Usar máscaras:

    - O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas.

    - Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

    - O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/`(delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.

    É possível excluir um objeto da verificação sem excluí-lo da lista de objetos no escopo de proteção. Para fazer isso, desmarque a caixa de seleção ao lado do objeto.

13. Salvar alterações.

Adicionar computadores confiáveis para criptografia externa de dados

Caso sua organização use criptografia externa de dados para troca de arquivos, será necessário criar uma lista de computadores confiáveis. O Kaspersky Embedded Systems Security não monitora a criptografia de dados de computadores confiáveis.

O serviço Login de Auditoria deve estar ativado para permitir a exclusão de endereços da proteção de pastas compartilhadas contra criptografia externa. Por padrão, o serviço Login de Auditoria é desativado (para obter informações detalhadas sobre a ativação do serviço Login de Auditoria, acesse o site da Microsoft).

A funcionalidade de exclusão de endereços da pasta de proteção compartilhada não funcionará em um computador remoto se o computador remoto tiver sido ligado antes da inicialização do Kaspersky Embedded Systems Security. Você pode reiniciar esse computador remoto depois que o Kaspersky Embedded Systems Security for iniciado para garantir que a funcionalidade de exclusão de endereços da proteção de pasta compartilhada funcione nesse computador remoto.

Como adicionar um computador confiável para criptografia externa de dados no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção do Computador em Tempo Real**.
4. Na seção **Detecção de Comportamento**, clique em **Configurações**.
5. Vá para a guia **Proteção de pastas compartilhadas**.
6. No bloco **Exclusões de endereço IP**, clique no botão **Configurar**.
7. Clique no botão **Adicionar** na janela que se abre.
8. Insira o endereço IP ou nome do computador a partir do qual as tentativas de criptografia externa não devem ser tratadas.
9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como adicionar um computador confiável para criptografia externa de dados no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção do Computador em Tempo Real** → **Detecção de Comportamento** e clique no botão **Configurar**.

   A janela **Detecção de Comportamento** é aberta.
5. Vá para a guia **Proteção de pastas compartilhadas**.
6. No bloco **Exclusões**, clique no botão **Adicionar**.
7. Insira o endereço IP ou nome do computador a partir do qual as tentativas de criptografia externa não devem ser tratadas.
8. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como adicionar um computador confiável para criptografia externa de dados no Console do Aplicativo

1. Na árvore do Kaspersky Embedded Systems Security Console, selecione **Proteção do Computador em Tempo Real** → **Detecção de Comportamento**.
2. No painel de resultados do nó **Detecção de Comportamento**, clique em **Propriedades**.

   Esse procedimento abre a janela **Propriedades: Detecção de Comportamento**.
3. Vá para a guia **Proteção de pastas compartilhadas**.
4. No bloco **Exclusões de endereço IP**, clique no botão **Configurar**.
5. Clique no botão **Adicionar** na janela que se abre.
6. Insira o endereço IP ou nome do computador a partir do qual as tentativas de criptografia externa não devem ser tratadas.
7. Salvar alterações.

Configurar o período de bloqueio de um computador não confiável

Um *computador não confiável* é um computador remoto que está envolvido em atividades maliciosas ou criptografia de dados. Por padrão, o Kaspersky Embedded Systems Security bloqueia a sessão de um usuário remoto por uma hora. Quando o período de bloqueio expira, o Kaspersky Embedded Systems Security remove o computador da lista de bloqueios e restaura o acesso à pasta compartilhada.

Como configurar o período de bloqueio de um computador não confiável no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção do Computador em Tempo Real**.
4. Na seção **Detecção de Comportamento**, clique em **Configurações**.
5. Marque ou desmarque a caixa de seleção **Detecção de Comportamento** para ativar ou desativar o componente.
6. Vá para a guia **Proteção de pastas compartilhadas**.
7. Em **Na detecção de criptografia externa de pastas compartilhadas**, configure o período de bloqueio de um computador não confiável que esteja envolvido em atividades maliciosas ou criptografia de dados.
8. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como configurar o período de bloqueio de um computador não confiável no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Proteção do Computador em Tempo Real** → **Detecção de Comportamento** e clique no botão **Configurar**.

   A janela **Detecção de Comportamento** é aberta.
5. Use a caixa de seleção **Ativar Detecção de Comportamento** para ativar ou desativar o componente.
6. Vá para a guia **Proteção de pastas compartilhadas**.

7. Em **Detecção de criptografia externa**, configure o período de bloqueio de um computador não confiável que esteja envolvido em atividades maliciosas ou criptografia de dados.
8. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como configurar o período de bloqueio de um computador não confiável no Console do Aplicativo

1. Na árvore do Kaspersky Embedded Systems Security Console, selecione **Proteção do Computador em Tempo Real → Detecção de Comportamento**.
2. No painel de resultados do nó **Detecção de Comportamento**, clique em **Propriedades**.

   Esse procedimento abre a janela **Propriedades: Detecção de Comportamento**.
3. Marque a caixa de seleção **Objetos a serem detectados**.
4. Vá para a guia **Proteção de pastas compartilhadas**.
5. Em **Proteção de pastas compartilhadas contra criptografia externa**, configure o período de bloqueio de um computador não confiável que esteja envolvido em atividades maliciosas ou criptografia de dados.
6. Salvar alterações.

Exportar e importar uma lista de exclusões da proteção de pastas compartilhadas contra criptografia externa

Você pode exportar a lista de exclusões para um arquivo XML. Em seguida, você pode modificar o arquivo para, por exemplo, adicionar um grande número de endereços do mesmo tipo. Você também pode usar a função de exportação/importação para fazer backup da lista de exclusões ou para migrar a lista para um servidor diferente.

Como exportar e importar uma lista de exclusões no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção do Computador em Tempo Real**.
4. Na seção **Detecção de Comportamento**, clique em **Configurações**.
5. Vá para a guia **Proteção de pastas compartilhadas**.
6. No bloco **Exclusões de endereço IP**, clique no botão **Configurar**.

7. Para exportar a lista de regras:

   a. Selecione as exclusões que deseja exportar.

   b. Clique no botão e selecione o modo de exportação: exportar a lista completa de exclusões ou apenas as exclusões selecionadas.

   c. Na janela exibida, especifique o nome do arquivo XML para o qual você quer exportar a lista de exclusões e selecione a pasta na qual você quer salvar esse arquivo.

   d. Salvar o arquivo.

      O Kaspersky Embedded Systems Security exporta toda a lista de regras para o arquivo XML.

8. Para importar a lista de exclusões:

   a. Clique no botão → **Importar**.

      Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de exclusões.

   b. Abra o arquivo.

      O Kaspersky Embedded Systems Security importa as exclusões.

9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como exportar e importar uma lista de exclusões no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Vá para **Proteção do Computador em Tempo Real** → **Detecção de Comportamento** e clique no botão **Configurar**.

   A janela **Detecção de Comportamento** é aberta.

5. Use a caixa de seleção **Ativar Detecção de Comportamento** para ativar ou desativar o componente.

6. Vá para a guia **Proteção de pastas compartilhadas**.

7. Para exportar a lista de exclusões, na seção **Exclusões**:

   a. Selecione as exclusões que deseja exportar.

   b. Clique no botão **Exportar** e selecione o modo de exportação: exportar a lista completa de exclusões ou apenas as exclusões selecionadas.

   c. Salvar o arquivo.

      O Kaspersky Embedded Systems Security exporta toda a lista de regras para o arquivo XML.

8. Para importar uma lista de exclusões, no bloco **Exclusões**:

   a. Clique no botão **Importar** e selecione um modo de importação: adicionar ou substituir.

   b. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de exclusões.

   c. Abra o arquivo.

      O Kaspersky Embedded Systems Security importa as exclusões de acordo com o modo selecionado.

9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Proteção Contra Ameaças à Rede

O componente Proteção Contra Ameaças à Rede verifica o tráfego de rede de entrada em busca de atividades típicas de ataques de rede. Ao detectar uma tentativa de ataque à rede direcionada ao computador, o Kaspersky Embedded Systems Security bloqueará a atividade de rede do computador invasor. As descrições dos tipos de ataques de rede atuais e formas de neutraliza-los estão disponibilizadas nos bancos de dados do aplicativo. A lista de ataques de rede que o componente Proteção Contra Ameaças à Rede detecta é atualizada durante atualizações de módulo do aplicativo e do banco de dados.

Por padrão, a tarefa *Proteção Contra Ameaças à Rede* é executada no modo **Bloquear**. Nesse modo, o Kaspersky Embedded Systems Security bloqueia conexões com computadores que apresentam atividades típicas de ataques de rede, podendo, em alguns casos, adicionar seus endereços IP à lista de sessões de rede bloqueadas.

Você pode visualizar a lista de hosts bloqueados no Armazenamento de Hosts Bloqueados.

O Kaspersky Embedded Systems Security limpa a lista de bloqueio quando o aplicativo é reiniciado e quando as configurações de proteção contra ameaças à rede são alteradas.

É possível restaurar o acesso aos hosts bloqueados e especificar quantos dias, horas e minutos após o bloqueio eles podem recuperar o acesso aos recursos de arquivos configurando o 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 está desinstalado.
- O endereço IP foi excluído manualmente da lista de hosts bloqueados.
- O prazo de bloqueio do host expirou.
- O modo **Bloquear** foi desligado.

Como ativar e configurar a Proteção Contra Ameaças à Rede no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados**.
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 de propriedades da política, acesse a seção **Controle de atividades de rede**.
6. No bloco **Proteção Contra Ameaças à Rede**, clique no botão **Configurações**.

   A janela **Proteção Contra Ameaças à Rede** é exibida na guia **Geral**.

7. Use a caixa de seleção **Proteção Contra Ameaças à Rede** para ativar ou desativar o componente Proteção Contra Ameaças à Rede .

8. Selecione o modo de tarefa na seção **Modo de operação**:

   - **Bloquear**. Se esse modo for selecionado, o Kaspersky Embedded Systems Security analisará o tráfego de rede de entrada em busca de atividades típicas de ataques de rede, bloqueará a conexão com computadores que apresentem essa atividade e, em alguns casos, adicionará seus endereços IP à lista de sessões de rede bloqueadas. O aplicativo também registra eventos no log do componente sobre atividades detectadas que possuem características de ataques de rede.

   - **Informar**. Se esse modo for selecionado, o Kaspersky Embedded Systems Security analisará o tráfego de rede de entrada em busca de atividades típicas de ataques de rede, mas não bloqueará a conexão com computadores que apresentem essa atividade nem adicionará seus endereços IP à lista de sessões de rede bloqueadas. O aplicativo registra no log do componente os eventos relacionados à atividade detectada como típica de ataques de rede.

9. Use a caixa de seleção **Considerar verificação de portas e a saturação da rede como ataques** para ativar ou desativar a detecção dos ataques correspondentes.

10. Caso seja necessário, marque a caixa de seleção **Bloquear dispositivos de ataque por N min**.

11. Na seção **Proteção contra MAC spoofing**, marque ou desmarque a caixa de seleção **Ativar a proteção contra os ataques de MAC spoofing**.

12. Caso seja necessário, é possível **adicionar exclusões do bloqueio**.

    O Kaspersky Embedded Systems Security pode reconhecer um ataque de rede e bloquear uma conexão de rede não segura que esteja transmitindo um grande número de pacotes (por exemplo, de câmeras de vigilância). Para trabalhar com dispositivos confiáveis, você pode adicionar os endereços IP desses dispositivos à lista de exclusões. Também é possível selecionar o protocolo e a porta usados para comunicação e permitir atividades de rede específicas.

    A capacidade de selecionar protocolos e portas para exclusões foi adicionada ao Kaspersky Embedded Systems Security 4.0. Certifique-se de que o aplicativo e o plug-in de gerenciamento estejam atualizados para a versão 4.0 ou posterior. Se uma versão anterior do aplicativo ou do plug-in de gerenciamento estiver sendo utilizada, o Kaspersky Embedded Systems Security pode permitir atividades de rede apenas pelo endereço IP.

    a. Selecione a guia **Exclusões**.

    b. Marque a caixa de seleção **Não controlar endereços excluídos** para impedir que o Kaspersky Embedded Systems Security verifique o tráfego de rede de entrada em busca de endereços IP excluídos.

    c. Clique **Adicionar**.

    d. Na janela **Exclusões** , insira o endereço IP do computador a partir do qual os ataques de rede não devem ser bloqueados.

    e. Se necessário, selecione o protocolo e as portas pelas quais os dados são transmitidos.

f. Clique **OK**.

g. Execute as etapas c a f para cada exclusão adicionada.

13. Salvar alterações.

Como ativar e configurar a Proteção Contra Ameaças à Rede no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o nó **Proteção do Computador em Tempo Real → Proteção Contra Ameaças à Rede**.
2. Clique no link **Propriedades** no painel de resultados.

   A janela **Propriedades: Proteção Contra Ameaças à Rede** é aberta.
3. Marque a caixa de seleção **Proteção Contra Ameaças à Rede** para ativar o componente Proteção Contra Ameaças à Rede.
4. Selecione o modo de tarefa na seção **Modo de operação**:

   - **Bloquear**. Se esse modo for selecionado, o Kaspersky Embedded Systems Security analisará o tráfego de rede de entrada em busca de atividades típicas de ataques de rede, bloqueará a conexão com computadores que apresentem essa atividade e, em alguns casos, adicionará seus endereços IP à lista de sessões de rede bloqueadas. O aplicativo também registra eventos no log do componente sobre atividades detectadas que possuem características de ataques de rede.
   - **Informar**. Se esse modo for selecionado, o Kaspersky Embedded Systems Security analisará o tráfego de rede de entrada em busca de atividades típicas de ataques de rede, mas não bloqueará a conexão com computadores que apresentem essa atividade nem adicionará seus endereços IP à lista de sessões de rede bloqueadas. O aplicativo registra no log do componente os eventos relacionados à atividade detectada como típica de ataques de rede.
5. Use a caixa de seleção **Considerar verificação de portas e a saturação da rede como ataques** para ativar ou desativar a detecção dos ataques correspondentes.
6. Caso seja necessário, marque a caixa de seleção **Bloquear dispositivos de ataque por N min**.
7. Na seção **Proteção contra MAC spoofing**, marque ou desmarque a caixa de seleção **Ativar a proteção contra os ataques de MAC spoofing**.
8. Caso seja necessário, é possível **adicionar exclusões do bloqueio**.

   O Kaspersky Embedded Systems Security pode reconhecer um ataque de rede e bloquear uma conexão de rede não segura que esteja transmitindo um grande número de pacotes (por exemplo, de câmeras de vigilância). Para trabalhar com dispositivos confiáveis, você pode adicionar os endereços IP desses dispositivos à lista de exclusões. Também é possível selecionar o protocolo e a porta usados para comunicação e permitir atividades de rede específicas.

A capacidade de selecionar protocolos e portas para exclusões foi adicionada ao Kaspersky Embedded Systems Security 4.0. Certifique-se de que o aplicativo e o plug-in de gerenciamento estejam atualizados para a versão 4.0 ou posterior. Se uma versão anterior do aplicativo ou do plug-in de gerenciamento estiver sendo utilizada, o Kaspersky Embedded Systems Security pode permitir atividades de rede apenas pelo endereço IP.

a. Selecione a guia **Exclusões**.

b. Marque a caixa de seleção **Não controlar endereços excluídos** para impedir que o Kaspersky Embedded Systems Security verifique o tráfego de rede de entrada em busca de endereços IP excluídos.

c. Clique **Adicionar**.

d. Na janela **Exclusões** , insira o endereço IP do computador a partir do qual os ataques de rede não devem ser bloqueados.

e. Se necessário, selecione o protocolo e as portas pelas quais os dados são transmitidos.

f. Clique **OK**.

g. Execute as etapas c a f para cada exclusão adicionada.

9. Salvar alterações.

Como ativar e configurar a Proteção Contra Ameaças à Rede no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Controle de atividades de rede** → **Proteção Contra Ameaças à Rede**.
5. Marque a caixa de seleção **Ativar proteção contra ameaças à rede** na guia **Geral** para ativar o componente Proteção Contra Ameaças à Rede.

6. Selecionar o modo de operação da tarefa:

   - **Bloquear**. Se esse modo for selecionado, o Kaspersky Embedded Systems Security analisará o tráfego de rede de entrada em busca de atividades típicas de ataques de rede, bloqueará a conexão com computadores que apresentem essa atividade e, em alguns casos, adicionará seus endereços IP à lista de sessões de rede bloqueadas. O aplicativo também registra eventos no log do componente sobre atividades detectadas que possuem características de ataques de rede.

   - **Informar**. Se esse modo for selecionado, o Kaspersky Embedded Systems Security analisará o tráfego de rede de entrada em busca de atividades típicas de ataques de rede, mas não bloqueará a conexão com computadores que apresentem essa atividade nem adicionará seus endereços IP à lista de sessões de rede bloqueadas. O aplicativo registra no log do componente os eventos relacionados à atividade detectada como típica de ataques de rede.

7. Use a caixa de seleção **Considerar verificação de portas e a saturação da rede como ataques** para ativar ou desativar a detecção dos ataques correspondentes.

8. Caso seja necessário, marque a caixa de seleção **Bloquear dispositivos de ataque por N min**.

9. Selecione ou desmarque a caixa de seleção **Ativar a proteção contra os ataques de MAC spoofing**.

10. Caso seja necessário, é possível **adicionar exclusões do bloqueio**.

    O Kaspersky Embedded Systems Security pode reconhecer um ataque de rede e bloquear uma conexão de rede não segura que esteja transmitindo um grande número de pacotes (por exemplo, de câmeras de vigilância). Para trabalhar com dispositivos confiáveis, você pode adicionar os endereços IP desses dispositivos à lista de exclusões. Também é possível selecionar o protocolo e a porta usados para comunicação e permitir atividades de rede específicas.

    A capacidade de selecionar protocolos e portas para exclusões foi adicionada ao Kaspersky Embedded Systems Security 4.0. Certifique-se de que o aplicativo e o plug-in de gerenciamento estejam atualizados para a versão 4.0 ou posterior. Se uma versão anterior do aplicativo ou do plug-in de gerenciamento estiver sendo utilizada, o Kaspersky Embedded Systems Security pode permitir atividades de rede apenas pelo endereço IP.

    a. Selecione a guia **Exclusões**.

    b. Marque a caixa de seleção **Não controlar endereços excluídos** para impedir que o Kaspersky Embedded Systems Security verifique o tráfego de rede de entrada em busca de endereços IP excluídos.

    c. Clique **Adicionar**.

    d. Na janela **Exclusões** , insira o endereço IP do computador a partir do qual os ataques de rede não devem ser bloqueados.

    e. Se necessário, selecione o protocolo e as portas pelas quais os dados são transmitidos.

    f. Clique **OK**.

    g. Execute as etapas c a f para cada exclusão adicionada.

11. Salvar alterações.

Scanner AMSI

Quando a tarefa Verificador AMSI está em execução, o Kaspersky Embedded Systems Security controla a execução de scripts criados com o uso das 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 Antimalware Scan Interface (AMSI) instalada.

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 da Microsoft.

Nas configurações de componentes, é possível permitir ou negar a execução de scripts perigosos. Caso o Kaspersky Embedded Systems Security identifique um script como perigoso, ele bloqueia ou permite a sua execução de acordo com a ação selecionada. Caso a ação **Bloquear** seja selecionada, o aplicativo bloqueará os scripts perigosos e permitirá outros scripts.

O Kaspersky Embedded Systems Security é compatível com a tecnologia AMSI no Microsoft Windows 10, Microsoft Windows Server 2016 e posteriores.

Ativar e desativar a proteção AMSI

Como ativar ou desativar o AMSI Scanner no Console de Administração do Kaspersky Security Center

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

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

   b. Selecione o grupo de administração para o qual você deseja configurar a tarefa.

   c. Selecione a etiqueta **de políticas**.

   d. Abra a janela de propriedades da política com um clique duplo no nome da política.

   e. Na janela de propriedades da política, acesse a seção **Proteção do Computador em Tempo Real**.

   f. No bloco **AMSI Scanner**, clique no botão **Configurações**.
   A janela **AMSI Scanner** é exibida na guia **Geral**.

2. Execute uma das seguintes ações:

   - Marque a caixa de seleção **AMSI Scanner** caso queira ativar o AMSI Scanner.
   - Desmarque a caixa de seleção **AMSI Scanner** caso queira desativar o AMSI Scanner.

3. Na janela **AMSI Scanner**, clique no botão **OK**.

4. Clique no botão **OK** na janela **Propriedades: <Nome da política>**.

Como ativar o AMSI Scanner no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, selecione o node **Proteção do Computador em Tempo Real → AMSI Scanner**.

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

   A janela **AMSI Scanner** é exibida na guia **Geral**.

3. Execute uma das seguintes ações:

   - Marque a caixa de seleção **AMSI Scanner** caso queira ativar o AMSI Scanner.
   - Desmarque a caixa de seleção **AMSI Scanner** caso queira desativar o AMSI Scanner.

4. Na janela **AMSI Scanner**, clique no botão **OK**.

Como ativar o Verificador AMSI no Kaspersky Security Center Web Console

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

   a. Na janela principal do Web Console, selecione **Ativos (dispositivos) → Políticas e perfis**.

   b. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

   d. Selecione a seção **Proteção do Computador em Tempo Real**.

   e. No bloco **AMSI Scanner**, clique no botão **Configurar**.

   A janela **AMSI Scanner** é aberta.

2. Execute uma das seguintes ações:

   - Marque a caixa de seleção **AMSI Scanner** caso queira ativar o AMSI Scanner.
   - Desmarque a caixa de seleção **AMSI Scanner** caso queira desativar o AMSI Scanner.

3. Clique no botão **OK** na subseção **AMSI Scanner**.

4. Na janela **<Nome da política>**, clique em **Salvar**.

Configurações de Proteção AMSI

Como definir as configurações do AMSI Scanner no Console de Administração do Kaspersky Security Center

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

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

   b. Selecione o grupo de administração para o qual você deseja configurar a tarefa.

   c. Selecione a etiqueta **de políticas**.

   d. Abra a janela de propriedades da política com um clique duplo no nome da política.

   e. Na janela de propriedades da política, acesse a seção **Proteção do Computador em Tempo Real**.

   f. No bloco **AMSI Scanner**, clique no botão **Configurações**.

   A janela **AMSI Scanner** é exibida na guia **Geral**.

2. Selecione a ação que deseja que o Kaspersky Embedded Systems Security execute quando um script perigoso for executado:

   - **Informar**. O aplicativo permite a execução de scripts potencialmente perigosos. Um evento correspondente é registrado no log de tarefas.
   - **Bloquear**. O aplicativo bloqueia a execução de scripts potencialmente perigosos.

3. No bloco **Verificação de arquivos compostos**, especifique os tipos de arquivos compostos que deseja verificar: arquivos compactados, pacote de distribuição ou arquivos em formatos do Office.

4. No bloco **Limite de tamanho**, execute uma das seguintes ações:

   - Para impedir que o componente de AMSI Scanner descompacte grandes arquivos compostos, marque a caixa de seleção **Não descompactar arquivos compostos grandes** e especifique o valor necessário no campo **Tamanho máximo de arquivo (MB)**. O componente de AMSI Scanner não descompactará arquivos compostos maiores do que o tamanho especificado.
   - Para permitir que o componente de AMSI Scanner descompacte grandes arquivos compostos, desmarque a caixa de seleção **Não descompactar arquivos compostos grandes**.

   O componente de AMSI Scanner verifica os arquivos grandes que foram extraídos dos arquivos, mesmo se a caixa de seleção **Não descompactar arquivos compostos grandes** estiver marcada.

5. Na janela **AMSI Scanner**, clique no botão **OK**.

6. Clique no botão **OK** na janela **Propriedades: <Nome da política>**.

Como definir as configurações do AMSI Scanner no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, selecione o node **Proteção do Computador em Tempo Real → AMSI Scanner**.

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

   A janela **AMSI Scanner** é exibida na guia **Geral**.

3. Selecione a ação que deseja que o Kaspersky Embedded Systems Security execute quando um script perigoso for executado:

   - **Informar**. O aplicativo permite a execução de scripts potencialmente perigosos. Um evento correspondente é registrado no log de tarefas.

   - **Bloquear**. O aplicativo bloqueia a execução de scripts potencialmente perigosos.

4. No bloco **Verificação de arquivos compostos**, especifique os tipos de arquivos compostos que deseja verificar: arquivos compactados, pacote de distribuição ou arquivos em formatos do Office.

5. No bloco **Limite de tamanho**, execute uma das seguintes ações:

   - Para impedir que o componente de AMSI Scanner descompacte grandes arquivos compostos, marque a caixa de seleção **Não descompactar arquivos compostos grandes** e especifique o valor necessário no campo **Tamanho máximo de arquivo (MB)**. O componente de AMSI Scanner não descompactará arquivos compostos maiores do que o tamanho especificado.

   - Para permitir que o componente de AMSI Scanner descompacte grandes arquivos compostos, desmarque a caixa de seleção **Não descompactar arquivos compostos grandes**.

   O componente de AMSI Scanner verifica os arquivos grandes que foram extraídos dos arquivos, mesmo se a caixa de seleção **Não descompactar arquivos compostos grandes** estiver marcada.

6. Na janela **AMSI Scanner**, clique no botão **OK**.

Como definir as configurações do AMSI Scanner no Kaspersky Security Center Web Console

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

   a. Na janela principal do Web Console, selecione **Ativos (dispositivos) → Políticas e perfis**.

   b. Clique no nome da política do Kaspersky Embedded Systems Security.

      A janela de propriedades da política é exibida.

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

d. Selecione a seção **Proteção do Computador em Tempo Real**.

e. No bloco **AMSI Scanner**, clique no botão **Configurar**.

A janela **AMSI Scanner** é aberta.

2. Selecione a ação que deseja que o Kaspersky Embedded Systems Security execute quando um script perigoso for executado:

   - **Informar**. O aplicativo permite a execução de scripts potencialmente perigosos. Um evento correspondente é registrado no log de tarefas.
   - **Bloquear**. O aplicativo bloqueia a execução de scripts potencialmente perigosos.

3. No bloco **Verificação de arquivos compostos**, especifique os tipos de arquivos compostos que deseja verificar: arquivos compactados, pacote de distribuição ou arquivos em formatos do Office.

4. No bloco **Limite de tamanho**, execute uma das seguintes ações:

   - Para impedir que o componente de AMSI Scanner descompacte grandes arquivos compostos, marque a caixa de seleção **Não descompactar arquivos compostos grandes** e especifique o valor necessário no campo **Tamanho máximo de arquivo (MB)**. O componente de AMSI Scanner não descompactará arquivos compostos maiores do que o tamanho especificado.
   - Para permitir que o componente de AMSI Scanner descompacte grandes arquivos compostos, desmarque a caixa de seleção **Não descompactar arquivos compostos grandes**.

   O componente de AMSI Scanner verifica os arquivos grandes que foram extraídos dos arquivos, mesmo se a caixa de seleção **Não descompactar arquivos compostos grandes** estiver marcada.

5. Clique no botão **OK** na subseção **AMSI Scanner**.

6. Na janela **<Nome da política>**, clique em **Salvar**.

Controle de Inicialização de Aplicativos

Durante a execução da tarefa de Controle de Inicialização de Aplicativos, o Kaspersky Embedded Systems Security 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.

É possível permitir a inicialização de aplicativos com a criação de regras de permissão do Controle de Inicialização de Aplicativos.

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:

- **Bloquear**. O Kaspersky Embedded Systems Security controlará a inicialização de aplicativos usando regras de Controle de Inicialização de Aplicativos. O escopo das regras de Controle de Inicialização de Aplicativos é especificado nas configurações gerais da tarefa Controle de Inicialização de Aplicativos. Caso um aplicativo satisfaça as Regras de Controle de Inicialização de Aplicativos, mas sem que nenhuma das regras corresponda ao escopo das regras de Controle de Inicialização de Aplicativos, esses aplicativos serão impedidos de ser executados.

  A execução de aplicativos que não estejam protegidos pelas Regras de Controle de Inicialização de Aplicativos é proibida.

  A tarefa de **Controle de Inicialização de Aplicativos** não poderá ser iniciada no modo Ativo se nenhuma regra de Controle de Inicialização de Aplicativos tiver sido criada ou se houver mais de 65.535 regras de Controle de Inicialização de Aplicativos para um dispositivo protegido.

- **Informar**. O Kaspersky Embedded Systems Security permitirá a inicialização de todos os aplicativos. Porém, serão registradas informações sobre todas as inicializações de aplicativos, as regras que abrangem os aplicativos inicializados e as ações que seriam executadas caso a tarefa estivesse sendo executada no modo **Bloquear**. Este modo está definido por padrão.

Ao criar as regras de Controle de Inicialização de Aplicativos, recomendamos assegurar que elas não bloqueiem a execução dos aplicativos do sistema operacional.

O Kaspersky Embedded Systems Security também intercepta processos iniciados sob o Windows Subsystem for 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 os aplicativos executados sob o Windows Subsystem for 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 aplicativos. Consequentemente, elas são chamadas de regras de *permissão* ou *negação*.

- 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*.

- Condições de acionamento da regra.

  As regras de Controle de Inicialização de Aplicativos regulam a inicialização dos arquivos que satisfaçam pelo menos a uma condição de acionamento especificada nas configurações da regra. Por exemplo, os arquivos executáveis são assinados com o *certificado digital*, têm o *Hash SHA256* especificado, estão localizados no *caminho* especificado e correspondem aos argumentos de *linha de comando*. É necessário adicionar pelo menos uma condição de acionamento de regra. Caso contrário, a regra de Controle de Inicialização de Aplicativos não será adicionada.

- Exclusões da regra.

  É possível configurar as exclusões para a regra de Controle de Inicialização de Aplicativos de acordo com os mesmos critérios das condições de acionamento da regra. 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.

- 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.

Ao criar regras de Controle de Inicialização de Aplicativos, recomendamos que as novas regras não bloqueiem a execução dos aplicativos do sistema operacional.

Gerenciando regras de Controle de Inicialização de Aplicativos

Você pode executar as seguintes ações com as regras de Controle de Inicialização de Aplicativos:

- Adicionar manualmente.
- Gerar e adicionar regras automaticamente.
- Excluir.

- Importar e exportar.
- Filtrar a lista de regras.

Sobre o Controle de Distribuição de Software

A geração do Controle de Inicialização de Aplicativos pode se tornar mais complicada caso queira controlar a distribuição do software. Por exemplo, talvez seja conveniente fazer isso em dispositivos protegidos nos quais o software instalado seja atualizado automaticamente com regularidade. 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 em cenários de distribuição de software, é possível usar o Controle de distribuição de software.

Um *pacote de instalação* (doravante referido como "pacote") representa um ou diversos aplicativos a ser instalado em um dispositivo protegido. Um pacote de instalação também pode conter atualizações e comandos individuais.

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 controla apenas o ciclo completo de distribuição do aplicativo e 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.

Para usar o Controle de distribuição de software, é necessário ativar a funcionalidade **Aplicar regras a arquivos executáveis** nas configurações gerais do Controle de Inicialização de Aplicativos.

Cache de distribuição de software

O Kaspersky Embedded Systems Security 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 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. Em seguida, por padrão, todos os arquivos que têm as informações salvas no cache de distribuição têm permissão para iniciar.

Você não pode analisar, excluir ou modificar manualmente o cache de distribuição por meio da interface de usuário. O cache é preenchido e controlado pelo Kaspersky Embedded Systems Security.

É possível exportar o cache de distribuição para um arquivo de configuração (no formato XML) ou excluir o cache de distribuição na linha de comando.

Para exportar o cache de distribuição para um arquivo de configuração, execute o seguinte comando:

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

Para excluir o cache de distribuição, execute o seguinte comando:

```
kavshell appcontrol /config /clearsdc
```

O Kaspersky Embedded Systems Security 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

Os arquivos e pacotes extraídos e criados por um pacote primário de distribuição confiável (no primeiro nível de aninhamento) herdam o atributo de confiabilidade quando as suas somas de verificação são adicionadas ao cache de distribuição no momento em que 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 exemplo, caso o test.msi, um pacote que contém vários pacotes e aplicativos, seja adicionado à lista de exclusões e a funcionalidade **Permitir a inicialização de todos os arquivos secundários como pacotes de distribuição confiáveis** seja ativada, 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.

Caso o pacote test.msi seja adicionado à lista de exclusões e a funcionalidade **Permitir a inicialização de todos os arquivos secundários como pacotes de distribuição confiáveis** esteja desativada, o aplicativo concede o atributo confiável somente aos pacotes e arquivos executáveis que foram extraídos diretamente do pacote confiável (no primeiro nível de aninhamento). 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.

Os arquivos extraídos manterão o atributo de confiabilidade após a reinicialização do sistema operacional.

Para remover o atributo de herança de todos os arquivos extraídos, é necessário excluir o cache de distribuição e desativar a funcionalidade **Permitir a inicialização de todos os arquivos secundários como pacotes de distribuição confiáveis** antes de executar o pacote de instalação confiável novamente.

Trabalhar com a lista de regras de Controle de Inicialização de Aplicativos

A lista de pacotes confiáveis do 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.

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.

É possível 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.

Você pode criar listas de regras de Controle de Inicialização de Aplicativos no lado do Kaspersky Security Center de duas maneiras:

- Uso da 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 do Gerador de Regras de Controle de Inicialização de Aplicativos contém as regras de permissão especificadas nas configurações da tarefa de Controle de Inicialização de Aplicativos antes do início da tarefa. Nenhuma regra será criada para os aplicativos que não tenham permissão para ser iniciados nas configurações de tarefa. A inicialização desses aplicativos é negada por padrão. Então, é possível importar manualmente a lista de regras criada para as configurações da tarefa Controle de Inicialização de Aplicativos na 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 agendada 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.

- De acordo com o relatório de eventos gerado no Kaspersky Security Center para a tarefa Controle de Inicialização de Aplicativos, em execução no modo *Informar*.

  Nesse cenário, o Kaspersky Embedded Systems Security não nega a inicialização de aplicativos. Em vez disso, com a execução do Controle de Inicialização de Aplicativos no modo *Informar*, 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 gerar uma lista atualizada de regras ao executar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos ou a tarefa de Controle de Inicialização de Aplicativos no modo *Informar* 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 usados na rede ao gerar listas de regras, recomendamos inicializar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos e a tarefa de Controle de Inicialização de Aplicativos no modo *Informar* 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.

Ativando e configurando o Controle de Inicialização de Aplicativos

Como ativar e definir as configurações gerais do Controle de Inicialização de Aplicativos no Console de Administração do Kaspersky Security Center

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

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

   b. Selecione o grupo de administração para o qual você deseja configurar a tarefa.

   c. Selecione a guia **Políticas**.

   d. Clique duas vezes no nome da política que você quer configurar.

   e. Na janela de propriedades da política, acesse a seção **Controle de atividades locais**.

   f. No bloco **Controle de Inicialização de Aplicativos**, clique no botão **Configurações**.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

2. Ative **Controle de Inicialização de Aplicativos** usando a caixa de seleção com o mesmo nome.

3. No bloco **Modo de operação para regras de bloqueio**, defina as seguintes configurações:

   - Tarefa modo de operação:

     - **Bloquear**. O Kaspersky Embedded Systems Security aplica todas as regras criadas de Controle de Inicialização de Aplicativos.

     - **Informar**. O Kaspersky Embedded Systems Security 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.

   - Repetir a ação realizada na primeira inicialização do arquivo em todas as inicializações subsequentes desse arquivo

   - Negar a inicialização de interpretadores de comando sem um comando a executar

4. No bloco **Escopo de uso da regra**, defina 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. Em **Monitoramento de certificado**, ative ou desative a funcionalidade **Ignorar a ausência do carimbo de tempo de uma assinatura ao validar certificados**.

6. Na janela **Controle de Inicialização de Aplicativos**, clique em **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security 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.

Como ativar e definir as configurações gerais do Controle de Inicialização de Aplicativos no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, selecione o node **Controle do Computador → Controle de Inicialização de Aplicativos**.

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

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

3. Ative **Controle de Inicialização de Aplicativos** usando a caixa de seleção com o mesmo nome.

4. No bloco **Modo de operação para regras de bloqueio**, defina as seguintes configurações:

   - Tarefa modo de operação:

     - **Bloquear**. O Kaspersky Embedded Systems Security aplica todas as regras criadas de Controle de Inicialização de Aplicativos.

     - **Informar**. O Kaspersky Embedded Systems Security 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.

   - Repetir a ação realizada na primeira inicialização do arquivo em todas as inicializações subsequentes desse arquivo.

   - Negar a inicialização de interpretadores de comando sem um comando a executar.

5. No bloco **Escopo de uso da regra**, defina 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.

6. Em **Monitoramento de certificado**, ative ou desative a funcionalidade Ignorar a ausência do carimbo de tempo de uma assinatura ao validar certificados.

7. Na janela **Controle de Inicialização de Aplicativos**, clique em **OK** para salvar as alterações.

O Kaspersky Embedded Systems Security 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.

Como ativar e definir as configurações gerais do Controle de Inicialização de Aplicativos no Kaspersky Security Center Web Console

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

   a. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

   b. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

   d. Selecione a seção **Controle de atividades locais**.

   e. No bloco **Controle de Inicialização de Aplicativos**, clique no botão **Configurar**.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

2. Ative **Controle de Inicialização de Aplicativos** usando a caixa de seleção com o mesmo nome.

3. No bloco **Modo de operação para regras de bloqueio**, defina as seguintes configurações:

   - Tarefa modo de operação:

     - **Bloquear**. O Kaspersky Embedded Systems Security aplica todas as regras criadas de Controle de Inicialização de Aplicativos.

     - **Informar**. O Kaspersky Embedded Systems Security 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.

   - **Repetir a ação realizada na primeira inicialização do arquivo em todas as inicializações subsequentes desse arquivo**.

   - **Negar a inicialização de interpretadores de comando sem um comando a executar**.

4. No bloco **Escopo de uso da regra**, defina 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. Em **Monitoramento de certificado**, ative ou desative a funcionalidade **Ignorar a ausência do carimbo de tempo de uma assinatura ao validar certificados**.

6. Na janela **Controle de Inicialização de Aplicativos**, clique em **OK** para salvar as alterações.

7. Salvar a política modificada.

O Kaspersky Embedded Systems Security 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

Como configurar o controle de distribuição de software no Console de Administração do Kaspersky Security Center

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

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

   b. Selecione o grupo de administração para o qual você deseja configurar a tarefa.

   c. Selecione a guia **Políticas**.

   d. Clique duas vezes no nome da política que você quer configurar.

   e. Na janela de propriedades da política, acesse a seção **Controle de atividades locais**.

   f. No bloco **Controle de Inicialização de Aplicativos**, clique no botão **Configurações**.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

2. Selecione a guia **Controle de distribuição de software**.

3. Ative a funcionalidade **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados**.

   É possível ativar a funcionalidade **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados** caso na guia **Geral**, a funcionalidade **Aplicar regras a arquivos executáveis** esteja ativada.

4. Caso seja necessário, desative a funcionalidade **Sempre permitir a distribuição de software via Windows Installer**.

   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.

5. Caso seja necessário, ative a funcionalidade **Sempre permitir a 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.

6. Adicionar arquivos executáveis e pacotes de instalação para os quais deseja permitir a inicialização:

- Adicionar manualmente.

  a. No menu de contexto da pasta **Adicionar**, selecione **Adicionar um pacote de distribuição**.

  b. Clique no botão **Procurar** na janela que se abre.

  c. Selecione o arquivo executável ou pacote de distribuição.

  Os campos em **Critérios de confiança** são preenchidos automaticamente com as informações sobre o arquivo selecionado.

  d. Caso seja necessário, ative a funcionalidade **Permitir a inicialização de todos os arquivos secundários como pacotes de distribuição confiáveis**.

  e. Selecione o critério que decidirá se o arquivo executável ou pacote de instalação é confiável: **Detalhes do certificado** ou **Hash SHA256**.

  f. Clique em **OK**.

  O arquivo executável ou o pacote de instalação é adicionado à lista.

- Adicionar diversos por hash

  a. No menu de contexto da pasta **Adicionar**, selecione **Adicionar diversos pacotes de distribuição por hash**.

  b. Uma janela será aberta; nessa janela, selecione qualquer número de arquivos ou pacotes de instalação.

  c. Clique em **Abrir**.

  Arquivos executáveis ou pacotes de instalação serão adicionados à lista. O Hash SHA256 foi especificado em suas propriedades.

- Importar do arquivo

  a. Clique **Importar**.

  b. Na janela aberta, selecione um arquivo .TXT com informações sobre arquivos executáveis e pacotes de instalação.

  c. Clique em **Abrir**.

  Arquivos executáveis ou pacotes de instalação serão adicionados à lista. O Hash SHA256 foi especificado em suas propriedades.

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 bloqueia a inicialização desse arquivo executável, mas considera o processo do arquivo executável como confiável.

7. Caso seja necessário, edite a lista de arquivos executáveis e pacotes de instalação adicionados clicando no botão **Editar**.
8. Caso seja necessário, remova os arquivos executáveis e os pacotes de instalação adicionados clicando no botão **Excluir**. Nesse caso, os arquivos executáveis descompactados têm permissão para serem executados.

   Para impedir a execução de arquivos executáveis descompactados, é necessário remover o Kaspersky Embedded Systems Security do dispositivo protegido ou criar regras de negação do Controle de Inicialização de Aplicativos para os arquivos descompactados.

9. Clique **OK**.

Como configurar o Controle de distribuição de software no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, selecione o node **Controle do Computador → Controle de Inicialização de Aplicativos**.
2. Clique no link **Propriedades** no painel de resultados.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.
3. Selecione a guia **Controle de distribuição de software**.
4. Ative a funcionalidade **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados**.

   É possível ativar a funcionalidade **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados** caso na guia **Geral**, a funcionalidade **Aplicar regras a arquivos executáveis** esteja ativada.
5. Caso seja necessário, desative a funcionalidade **Sempre permitir a distribuição de software via Windows Installer**.

   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.

6. Caso seja necessário, ative a funcionalidade **Sempre permitir a 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.

7. Adicionar arquivos executáveis e pacotes de instalação para os quais deseja permitir a inicialização:

   - **Adicionar manualmente.**

     a. No menu de contexto da pasta **Adicionar**, selecione **Adicionar um pacote de distribuição**.

     b. Clique no botão **Procurar** na janela que se abre.

     c. Selecione o arquivo executável ou pacote de distribuição.

     Os campos em **Critérios de confiança** são preenchidos automaticamente com as informações sobre o arquivo selecionado.

     d. Caso seja necessário, ative a funcionalidade **Permitir a inicialização de todos os arquivos secundários como pacotes de distribuição confiáveis**.

     e. Selecione o critério que decidirá se o arquivo executável ou pacote de instalação é confiável: **Detalhes do certificado** ou **Hash SHA256**.

     f. Clique em **OK**.

     O arquivo executável ou o pacote de instalação é adicionado à lista.

   - **Adicionar diversos por hash**

     a. No menu de contexto da pasta **Adicionar**, selecione **Adicionar diversos pacotes de distribuição por hash**.

     b. Uma janela será aberta; nessa janela, selecione qualquer número de arquivos ou pacotes de instalação.

     c. Clique em **Abrir**.

     Arquivos executáveis ou pacotes de instalação serão adicionados à lista. O Hash SHA256 foi especificado em suas propriedades.

- Importar do arquivo

  a. Clique **Importar**.

  b. Na janela aberta, selecione um arquivo .TXT com informações sobre arquivos executáveis e pacotes de instalação.

  c. Clique em **Abrir**.

  Arquivos executáveis ou pacotes de instalação serão adicionados à lista. O Hash SHA256 foi especificado em suas propriedades.

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 bloqueia a inicialização desse arquivo executável, mas considera o processo do arquivo executável como confiável.

8. Caso seja necessário, edite a lista de arquivos executáveis e pacotes de instalação adicionados clicando no botão **Editar**.
9. Caso seja necessário, remova os arquivos executáveis e os pacotes de instalação adicionados clicando no botão **Excluir**. Nesse caso, os arquivos executáveis descompactados têm permissão para serem executados.

Para impedir a execução de arquivos executáveis descompactados, é necessário remover o Kaspersky Embedded Systems Security do dispositivo protegido ou criar regras de negação do Controle de Inicialização de Aplicativos para os arquivos descompactados.

10. Clique **OK**.

Como configurar o Controle de distribuição de software no Kaspersky Security Center Web Console

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

   a. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

   b. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

   d. Selecione a seção **Controle de atividades locais**.

e. No bloco **Controle de Inicialização de Aplicativos**, clique no botão **Configurar**.

A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

2. Selecione a guia **Controle de distribuição de software**.

3. Ative a funcionalidade **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados**.

É possível ativar a funcionalidade **Permitir automaticamente a distribuição de software por meio dos aplicativos e pacotes listados** caso na guia **Geral**, a funcionalidade **Aplicar regras a arquivos executáveis** esteja ativada.

4. Caso seja necessário, desative a funcionalidade **Sempre permitir distribuição de software via Windows Installer**.

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.

5. Caso seja necessário, ative a funcionalidade **Sempre permitir a 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.

6. Adicionar arquivos executáveis e pacotes de instalação para os quais deseja permitir a inicialização:

- **Manualmente**

a. Clique no botão **Adicionar**.

b. Em **Critérios de confiança**, selecione o critério que decidirá se o arquivo executável ou pacote de instalação é confiável: **Usar certificado digital** ou **Usar hash SHA256**.

c. Caso tenha selecionado **Usar certificado digital**, insira o cabeçalho e a impressão digital do certificado com o qual o arquivo executável ou o pacote de instalação está assinado e também o nome do arquivo executável ou pacote de instalação.

d. Caso tenha selecionado **Usar hash SHA256**, clique em **Procurar** para selecionar o arquivo executável ou pacote de instalação.

e. Caso seja necessário, ative a funcionalidade **Permitir a inicialização de todos os arquivos secundários como pacotes de distribuição confiáveis**.

f. Clique em **OK**.

O arquivo executável ou o pacote de instalação é adicionado à lista.

- Importar do arquivo

  a. Clique **Importar**.

  b. Na janela aberta, selecione um arquivo .TXT com informações sobre arquivos executáveis e pacotes de instalação.

  c. Clique no botão **Abrir**.

  Arquivos executáveis ou pacotes de instalação serão adicionados à lista. O Hash SHA256 foi especificado em suas propriedades.

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 bloqueia a inicialização desse arquivo executável, mas considera o processo do arquivo executável como confiável.

7. Caso seja necessário, edite a lista de arquivos executáveis e pacotes de instalação adicionados clicando no botão **Editar**.
8. Caso seja necessário, remova os arquivos executáveis e os pacotes de instalação adicionados clicando no botão **Excluir**. Nesse caso, os arquivos executáveis descompactados têm permissão para serem executados.

   Para impedir a execução de arquivos executáveis descompactados, é necessário remover o Kaspersky Embedded Systems Security do dispositivo protegido ou criar regras de negação do Controle de Inicialização de Aplicativos para os arquivos descompactados.

9. Clique **OK**.
10. Clique no botão **OK** na subseção **Controle de Inicialização de Aplicativos**.

Trabalhar com a lista de regras de Controle de Inicialização de Aplicativos

Esta seção fornece instruções para a criação de uma lista de regras para o Controle de Inicialização de Aplicativos.

Adição de uma regra de Controle de Inicialização de Aplicativos

Como adicionar as regras de Controle de Inicialização de Aplicativos no Kaspersky Security Center Administration Console

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

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

   b. Selecione o grupo de administração para o qual você deseja configurar a tarefa.

   c. Selecione a guia **Políticas**.

   d. Clique duas vezes no nome da política que você quer configurar.

   e. Na janela de propriedades da política, acesse a seção **Controle de atividades locais**.

   f. No bloco **Controle de Inicialização de Aplicativos**, clique no botão **Configurações**.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

2. Selecione a guia **Regras**.

3. Na lista suspensa **Utilização da regra**, selecione a categoria do aplicativo criada.

   - **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.

   - **Substituir regras locais por regras de política**. O aplicativo aplica a lista de regras especificada na política para o Controle de Inicialização de Aplicativos em um grupo de dispositivos protegidos. As listas de regras locais não podem ser criadas, editas ou aplicadas.

4. Caso seja necessário, ative a funcionalidade Negar a modificação das regras locais feitas por usuários.

   Caso a funcionalidade esteja ativada, o aplicativo não permitirá a edição local das regras de Controle de Inicialização de Aplicativos no Console do Aplicativo. Essa função está desativada por padrão.

5. Adicione regras de Controle de Dispositivos de uma das seguintes formas:

   - Manualmente.

     a. Clique **Adicionar**.

     A janela **Controle de Inicialização de Aplicativos** é aberta.

     b. No campo **Nome**, insira ou edite o nome da regra.

     c. No campo **Descrição**, insira uma descrição da regra.

d. Na lista suspensa **Tipo**, selecione o tipo de regra:

- **Permissão** se quiser que a regra permita a execução dos aplicativos descritos por ela.
- **Proibição** se quiser que a regra bloqueie a inicialização dos aplicativos descritos por ela.

e. 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. Arquivos com as seguintes extensões são compatíveis: .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct.

f. Marque a caixa de seleção **Atualizadores confiáveis** se desejar que o Kaspersky Embedded Systems Security considere aplicativos que correspondam às condições de acionamento de regras como atualizadores confiáveis. Atualizadores confiáveis são aplicativos que têm permissão de criar outros arquivos executáveis que poderão ser executados posteriormente.

Caso um aplicativo acione várias regras, o Kaspersky Embedded Systems Security definirá o sinalizador *Atualizadores confiáveis* se as seguintes condições forem atendidas:

- Todas as regras permitem que o aplicativo seja executado.
- Pelo menos uma regra tem a caixa de seleção **Atualizadores confiáveis** marcada.

g. Adicionar condições de acionamento para a regra de Controle de Inicialização de Aplicativos.

h. Adicionar exclusões das condições de acionamento da regra de Controle de Inicialização de Aplicativos.

i. **Adicionar usuários e/ou grupos de usuários que têm permissão ou não para iniciar os aplicativos que satisfaçam a regra**.

a. Selecione a guia **Usuário ou grupo**.

b. No menu de contexto do botão **Adicionar**, selecione o método para adicionar usuários ou grupos.

c. O procedimento abre uma janela; nessa janela, digite ou selecione o nome de um usuário ou grupo de usuários.

d. Clique em **OK**.

e. Conclua as etapas b a d para cada usuário ou grupo de usuários.

j. Clique em **OK**.

- Pela importação de um arquivo XML contendo regras de Controle de Dispositivos

  a. No menu de contexto do botão selecione o item **Importar → Do arquivo XML**.

  b. Escolha como adicionar regras de Controle de Dispositivos de um arquivo XML àquelas disponíveis na política:

  - **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas.
  - **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
  - **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.

  c. Na janela que é aberta, especifique o caminho para o arquivo XML criado após a conclusão da tarefa local ou da tarefa de grupo para o Gerador de Regras de Controle de Inicialização de Aplicativos.

  d. Clique **Abrir**.

- De acordo com os eventos do Kaspersky Security Center que usam uma solicitação.

  a. No menu de contexto do botão selecione o item **Importar → Criar regras de permissão com base em eventos do Kaspersky Security Center (solicitação)**.

  b. 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 aberta.

  c. Selecione os tipos de eventos de acordo com os quais o aplicativo criará regras do Controle de Inicialização de Aplicativos:

  - **Inicialização do aplicativo negada**.
  - **Modo somente estatísticas: inicialização de aplicativos negada**.

  d. Selecione o período da lista suspensa **Solicitação de eventos que foram gerados dentro do período**.

e. 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 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 usa o certificado digital do arquivo para gerar a regra quando a soma de verificação e o certificado do arquivo estiverem disponíveis.

f. Clique **Gerar regras**.

g. Clique **OK**.

- Ao importar um arquivo TXT com a seleção de eventos de aplicativo bloqueada pelo Kaspersky Security Center.

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados**.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela de propriedades da política, acesse a seção **Registros e notificações**.
6. No bloco **Logs de tarefas**, clique no botão **Configurações**.

   A janela **Notificações** é aberta.
7. Expanda o nó **Controle de atividades locais**.
8. Selecione a seção **Controle de Inicialização de Aplicativos**.
9. Na lista de eventos do Controle de Inicialização de Aplicativos, na coluna **Enviar eventos ao Kaspersky Security Center**, marque as caixas de seleção ao lado de *Proibida a inicialização do aplicativo* e *Proibida a inicialização do aplicativo em modo de teste*.
10. Salvar alterações.
11. Na seção **Configuração de eventos** da política, verifique e confirme se o tempo de duração do armazenamento do evento especificado no campo **Armazenar no banco de dados do Servidor de Administração por (dias)** é maior que o período para o qual se planeja coletar as informações sobre as inicializações impedidas de aplicativos (o padrão é 30 dias).

    Depois que o período de retenção do log de Controle de Dispositivos expirar, os eventos registrados serão excluídos e não aparecerão no relatório.
12. Ativar a política configurada para coletar dados referentes a inicializações negadas de aplicativos.

13. Se necessário, modifique o modo do Controle de Dispositivos.

14. Quando o período de coleta de informações sobre as inicializações impedidas de aplicativos expirar, faça selecione eventos em *Proibida a inicialização do aplicativo* e *Proibida a inicialização do aplicativo em modo de teste* e exporte para um arquivo TXT. Para saber mais detalhes, consulte a seção "Seleções de eventos" na *Ajuda do Kaspersky Security Center*.

15. Abra o arquivo TXT exportado.

16. Caso seja necessário, edite a lista de eventos.

Antes de importar os dados dos aplicativos bloqueados, verifique e confirme se a lista que está sendo importada contém apenas os aplicativos que serão permitidos, e nada mais.

a. No menu de contexto do botão selecione o item **Importar → Criar regras de permissão com base no arquivo TXT com eventos selecionados do Kaspersky Security Center**.

b. Escolha como adicionar regras de Controle de Dispositivos de um relatório àquelas disponíveis na política:

- **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.

c. Na janela do sistema Windows aberta, especifique o caminho para o arquivo TXT para o qual os eventos do relatório do Kaspersky Security Center sobre dispositivos bloqueados foram exportados.

d. Clique **Abrir**.

As regras de Controle de Inicialização de Aplicativos adicionadas serão exibidas na lista.

6. Caso seja necessário, execute a etapa 5 para adicionar mais regras de Controle de Inicialização de Aplicativos.

7. Caso seja necessário, edite as regras de Controle de Inicialização de Aplicativos adicionadas ao clicar no botão **Editar**.

8. Caso seja necessário, exclua as regras de Controle de Inicialização de Aplicativos adicionadas clicando no botão **Excluir**.

9. Clique **OK**.

Como adicionar regras de Controle de Inicialização de Aplicativos no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, selecione o node **Controle do Computador** → **Controle de Inicialização de Aplicativos**.
2. Clique no link **Propriedades** no painel de resultados.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.
3. Selecione a guia **Regras**.
4. Adicione regras de Controle de Dispositivos de uma das seguintes formas:

   - Manualmente

     a. Clique **Adicionar**.

        A janela **Controle de Inicialização de Aplicativos** é aberta.

     b. No campo **Nome**, insira ou edite o nome da regra.

     c. No campo **Descrição**, insira uma descrição da regra.

     d. Na lista suspensa **Tipo**, selecione o tipo de regra:

        - **Permissão** se quiser que a regra permita a execução dos aplicativos descritos por ela.
        - **Proibição** se quiser que a regra bloqueie a inicialização dos aplicativos descritos por ela.

     e. 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. Arquivos com as seguintes extensões são compatíveis: .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct.

     f. Marque a caixa de seleção **Atualizadores confiáveis** se desejar que o Kaspersky Embedded Systems Security considere aplicativos que correspondam às condições de acionamento de regras como atualizadores confiáveis. Atualizadores confiáveis são aplicativos que têm permissão de criar outros arquivos executáveis que poderão ser executados posteriormente.

        Caso um aplicativo acione várias regras, o Kaspersky Embedded Systems Security definirá o sinalizador *Atualizadores confiáveis* se as seguintes condições forem atendidas:

        - Todas as regras permitem que o aplicativo seja executado.
        - Pelo menos uma regra tem a caixa de seleção **Atualizadores confiáveis** marcada.

     g. Adicionar condições de acionamento para a regra de Controle de Inicialização de Aplicativos.

     h. Adicionar exclusões das condições de acionamento da regra de Controle de Inicialização de Aplicativos.

i. Adicionar usuários e/ou grupos de usuários que têm permissão ou não para iniciar os aplicativos que satisfaçam a regra.

a. Selecione a guia **Usuário ou grupo**.

b. No menu de contexto do botão **Adicionar**, selecione o método para adicionar usuários ou grupos.

c. O procedimento abre uma janela; nessa janela, digite ou selecione o nome de um usuário ou grupo de usuários.

d. Clique em **OK**.

e. Conclua as etapas b a d para cada usuário ou grupo de usuários.

j. Clique em **OK**.

- Pela importação de um arquivo XML contendo regras de Controle de Dispositivos.

a. No menu de contexto do botão selecione o item **Importar** → **Do arquivo XML**.

b. Escolha como adicionar regras de Controle de Dispositivos de um arquivo XML àquelas disponíveis na política:

- **Substituir as regras existentes**, se quiser substituir as regras existentes pelas regras importadas.
- **Adicionar às regras existentes**, se quiser adicionar as regras importadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
- **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.

c. Na janela que é aberta, especifique o caminho para o arquivo XML criado após a conclusão da tarefa local ou da tarefa de grupo para o Gerador de Regras de Controle de Inicialização de Aplicativos.

d. Clique **Abrir**.

As regras de Controle de Inicialização de Aplicativos adicionadas serão exibidas na lista.

5. Caso seja necessário, execute a etapa 5 para adicionar mais regras de Controle de Inicialização de Aplicativos.

6. Caso seja necessário, edite as regras de Controle de Inicialização de Aplicativos adicionadas ao clicar no botão **Editar**.

7. Caso seja necessário, exclua as regras de Controle de Inicialização de Aplicativos adicionadas clicando no botão **Excluir**.

8. Clique **OK**.

Como adicionar regras de Controle de Inicialização de Aplicativos no Kaspersky Security Center Web Console

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

   a. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

   b. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

   d. Selecione a seção **Controle de atividades locais**.

   e. No bloco **Controle de Inicialização de Aplicativos**, clique no botão **Configurar**.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

2. Selecione a guia **Regras**.

3. Na lista suspensa **Aplicação de regras**, selecione a categoria do aplicativo criada.

   - **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.
   - **Substituir regras locais por regras de política**. O aplicativo aplica a lista de regras especificada na política para o Controle de Inicialização de Aplicativos em um grupo de dispositivos protegidos. As listas de regras locais não podem ser criadas, editas ou aplicadas.

4. Caso seja necessário, ative a funcionalidade **Negar a modificação das regras locais feitas por usuários**.

5. Adicione regras de Controle de Dispositivos de uma das seguintes formas:

   - Manualmente

     a. Clique **Adicionar**.

     A janela **Configurações de regra** é aberta.

     b. No campo **Nome**, insira ou edite o nome da regra.

     c. Na lista suspensa **Tipo**, selecione o tipo de regra:

     - **Permissão** se quiser que a regra permita a execução dos aplicativos descritos por ela.
     - **Proibição** se quiser que a regra bloqueie a inicialização dos aplicativos descritos por ela.

d. 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.

e. Marque a caixa de seleção **Negar para outros usuários** se quiser que o aplicativo bloqueie a inicialização dos aplicativos descritos pela regra para todos os usuários que não estão listados na guia **Usuário ou grupo**.

f. Marque a caixa de seleção **Atualizadores confiáveis** se desejar que o Kaspersky Embedded Systems Security considere aplicativos que correspondam às condições de acionamento de regras como atualizadores confiáveis. Atualizadores confiáveis são aplicativos que têm permissão de criar outros arquivos executáveis que poderão ser executados posteriormente.

Caso um aplicativo acione várias regras, o Kaspersky Embedded Systems Security definirá o sinalizador *Atualizadores confiáveis* se as seguintes condições forem atendidas:

- Todas as regras permitem que o aplicativo seja executado.
- Pelo menos uma regra tem a caixa de seleção **Atualizadores confiáveis** marcada.

g. Adicionar condições de acionamento para a regra de Controle de Inicialização de Aplicativos.

h. Adicionar exclusões das condições de acionamento da regra de Controle de Inicialização de Aplicativos.

i. **Adicionar usuários e/ou grupos de usuários que têm permissão ou não para iniciar os aplicativos que satisfaçam a regra**.

a. Selecione a guia **Usuário ou grupo**.

b. Clique **Adicionar**.

c. O procedimento abre uma janela; nessa janela, digite ou selecione o nome de um usuário ou grupo de usuários.

d. Clique **Selecionar**.

e. Conclua as etapas b a d para cada usuário ou grupo de usuários.

j. Clique em **OK**.

As regras de Controle de Inicialização de Aplicativos adicionadas serão exibidas na lista.

- **Pela importação de um arquivo XML contendo regras de Controle de Dispositivos.**

a. Clique **Importar**.

b. No bloco **Importar do arquivo**, clique no botão **Selecionar**.

c. Especifique o caminho para o arquivo XML criado após a conclusão da tarefa local ou da tarefa de grupo para o Gerador de Regras de Controle de Inicialização de Aplicativos.

d. Clique **Abrir**.

e. Clique **Importar**.

As regras são adicionadas 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.

- Ao importar um arquivo XML que contém as regras de Controle de Inicialização de Aplicativos do Kaspersky Embedded Systems Security 4.0.

  a. Clique **Importar da versão anterior**.

  b. No bloco **Importar do arquivo**, clique no botão **Selecionar**.

  c. Especifique o caminho para o arquivo XML com as regras de Controle de Inicialização de Aplicativos exportado do Kaspersky Embedded Systems Security 4.0.

  d. Clique em **Abrir**.

  e. Clique **Importar**.

  As regras são adicionadas 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.

- Ao importar regras de um arquivo de relatório do Kaspersky Security Center.

  a. Clique **Importar do relatório KSC**.

  b. Na janela que é aberta, selecione o arquivo TXT para o qual os eventos do relatório foram exportados.

  c. Clique em **Abrir**.

  As regras baseadas no relatório do Kaspersky Security Center são adicionadas à lista de regras da política.

- De acordo com os eventos do Kaspersky Security Center que usam uma solicitação

  a. Clique **Permissão de regras a partir de eventos KSC**.

  A janela **Gerador de Regras de Controle de Inicialização de Aplicativos** é aberta.

b. Selecione os tipos de eventos de acordo com os quais o aplicativo criará regras do Controle de Inicialização de Aplicativos:

- **Todos os eventos**.
- **Inicialização do aplicativo negada**.
- **Modo somente estatísticas: inicialização de aplicativos negada**.

c. Selecione o período da lista suspensa **Usar os eventos gerados dentro do período**.

d. 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 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 usa o certificado digital do arquivo para gerar a regra quando a soma de verificação e o certificado do arquivo estiverem disponíveis.

e. Caso seja necessário, especifique o nome do grupo de dispositivos gerenciados no campo **Usar os eventos gerados para um grupo de dispositivos gerenciados**.

f. Clique **Gerar regras**.

g. Na lista suspensa **Regra para adicionar na lista principal**, selecione o princípio para adicionar as regras na 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.

h. Selecione as regras que deseja exportar para as regras de Controle de Inicialização de Aplicativos da política e clique no botão **Exportar**.

i. Salvar alterações.

6. Caso seja necessário, execute a etapa 5 para adicionar mais regras de Controle de Inicialização de Aplicativos.
7. Caso seja necessário, edite as regras de Controle de Inicialização de Aplicativos adicionadas ao clicar no botão **Editar**.
8. Caso seja necessário, exclua as regras de Controle de Inicialização de Aplicativos adicionadas clicando no botão **Excluir**.
9. Clique **OK**.

Adicionar uma condição de acionamento para a regra de Controle de Aplicativos

Como adicionar condições de acionamento para a regra de Controle de Inicialização de Aplicativos no Console de Administração do Kaspersky Security Center

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

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

   b. Selecione o grupo de administração para o qual você deseja configurar a tarefa.

   c. Selecione a guia **Políticas**.

   d. Clique duas vezes no nome da política que você quer configurar.

   e. Na janela de propriedades da política, acesse a seção **Controle de atividades locais**.

   f. No bloco **Controle de Inicialização de Aplicativos**, clique no botão **Configurações**.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

2. Selecione a guia **Regras**.

3. Execute uma das seguintes ações:

   a. Clique no botão **Adicionar** caso esteja adicionando uma nova regra de Controle de Inicialização de Aplicativos.

   b. Na lista de regras de Controle de Inicialização de Aplicativos, selecione a regra para a qual deseja adicionar as condições de acionamento e clique no botão **Editar**.

   A janela **Controle de Inicialização de Aplicativos** é aberta.

4. Na guia **Condições**, no menu de contexto do botão **Adicionar**, selecione uma condição de acionamento para a regra de Controle de Inicialização de Aplicativos:

   - **Informações do arquivo**. As informações do arquivo selecionado serão usadas com a condição de acionamento da regra.

     a. Clique no botão **Procurar** na subseção **Informações do arquivo**.

     A janela padrão do Microsoft Windows **Open File** é exibida.

     b. Selecione o arquivo.

c. Clique em **Abrir**.

As informações sobre o arquivo selecionado serão exibidas na janela **Informações do arquivo**.

d. Selecione pelo menos uma opção:

- **Detalhes do certificado**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos assinados com um certificado digital que tenha os dados especificados.
- **Metadados**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham os metadados especificados.
- **Hash do arquivo**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham o hash SHA256 especificado.
- **Caminho do arquivo**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos no caminho especificado.

e. Caso seja necessário, no campo **Linha de comando**, insira o comando para iniciar o aplicativo na linha de comando. A regra controla a inicialização desse aplicativo. É possível usar os caracteres ? e * para inserir uma máscara.

> O Kaspersky Embedded Systems Security não reconhece caminhos que contêm barras ("/"). Use o caractere de barra invertida ("\") nos caminhos.

f. Clique **OK**.

- **Tipo de unidade**. A regra controla a inicialização de aplicativos de todas as unidades removíveis conectadas ao computador protegido.
- **Categoria KL**. A regra controla a inicialização de aplicativos pertencentes às categorias KL selecionadas.
- **Confiável pela KSN**. A regra controla o inicialização de aplicativos confiáveis na KSN.
- **Não confiável pela KSN**. A regra controla o inicialização de aplicativos não confiáveis na KSN.
- **Confiável pelo SO**. A regra controla a inicialização de aplicativos confiáveis no sistema operacional.

A exclusão será exibida na lista.

5. Caso seja necessário, execute a etapa anterior das instruções para cada uma das condições de acionamento da regra subsequente.
6. Caso seja necessário, edite as condições de acionamento da regra clicando no botão **Editar**.
7. Salvar alterações.

Como adicionar condições de acionamento para a regra de Controle de Inicialização de Aplicativos no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, selecione o node **Controle do Computador** → **Controle de Inicialização de Aplicativos**.
2. Clique no link **Propriedades** no painel de resultados.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.
3. Selecione a guia **Regras**.
4. Execute uma das seguintes ações:

   a. Clique no botão **Adicionar** caso esteja adicionando uma nova regra de Controle de Inicialização de Aplicativos.

   b. Na lista de regras de Controle de Inicialização de Aplicativos, selecione a regra para a qual deseja adicionar as condições de acionamento e clique no botão **Editar**.

   A janela **Controle de Inicialização de Aplicativos** é aberta.
5. Na guia **Condições**, no menu de contexto do botão **Adicionar**, selecione uma condição de acionamento para a regra de Controle de Inicialização de Aplicativos:

   - **Informações do arquivo**. As informações do arquivo selecionado serão usadas com a condição de acionamento da regra.

     a. Clique no botão **Procurar** na subseção **Informações do arquivo**.

     A janela padrão do Microsoft Windows **Open File** é exibida.

     b. Selecione o arquivo.

     c. Clique em **Abrir**.

     As informações sobre o arquivo selecionado serão exibidas na janela **Informações do arquivo**.

     d. Selecione pelo menos uma opção:

     - **Detalhes do certificado**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos assinados com um certificado digital que tenha os dados especificados.
     - **Metadados**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham os metadados especificados.
     - **Hash do arquivo**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham o hash SHA256 especificado.
     - **Caminho do arquivo**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos no caminho especificado.

e. Caso seja necessário, no campo **Linha de comando**, insira o comando para iniciar o aplicativo na linha de comando. A regra controla a inicialização desse aplicativo. É possível usar os caracteres ? e * para inserir uma máscara.

> O Kaspersky Embedded Systems Security não reconhece caminhos que contêm barras ("/"). Use o caractere de barra invertida ("\") nos caminhos.

f. Clique **OK**.

- **Tipo de unidade**. A regra controla a inicialização de aplicativos de todas as unidades removíveis conectadas ao computador protegido.
- **Categoria KL**. A regra controla a inicialização de aplicativos pertencentes às categorias KL selecionadas.
- **Confiável pela KSN**. A regra controla o inicialização de aplicativos confiáveis na KSN.
- **Não confiável pela KSN**. A regra controla o inicialização de aplicativos não confiáveis na KSN.
- **Confiável pelo SO**. A regra controla a inicialização de aplicativos confiáveis no sistema operacional.

A exclusão será exibida na lista.

6. Caso seja necessário, execute a etapa anterior das instruções para cada uma das condições de acionamento da regra subsequente.
7. Caso seja necessário, edite as condições de acionamento da regra clicando no botão **Editar**.
8. Salvar alterações.

Como adicionar condições de acionamento para a regra de Controle de Inicialização de Aplicativos no Kaspersky Security Center Web Console

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

   a. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

   b. Clique no nome da política do Kaspersky Embedded Systems Security.
   A janela de propriedades da política é exibida.

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

   d. Selecione a seção **Controle de atividades locais**.

   e. No bloco **Controle de Inicialização de Aplicativos**, clique no botão **Configurar**.
   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

2. Selecione a guia **Regras**.

3. Clique **Adicionar**.

   A janela **Configurações de regra** é aberta.

4. Na guia **Condições**, clique no botão **Adicionar**.

   A janela **Configurações de regra** é aberta.

5. Selecione as condições de acionamento para a regra de Controle de Aplicativos:

   - **Informações do arquivo**. As informações do arquivo serão usadas com a condição de acionamento da regra.

     a. Em **Critérios de acionamento de regras**, especifique o valor para pelo menos um critério:

     - **Certificado digital**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos assinados com um certificado digital que tenha os dados especificados.
     - **Metadados**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham os metadados especificados.
     - **Hash SHA256**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham o hash SHA256 especificado.
     - **Caminho do arquivo**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos no caminho especificado.

     b. Clique **OK**.

   - **Da categoria KL**. A regra controla a inicialização de aplicativos pertencentes às categorias KL selecionadas.
   - **Unidade removível**. A regra controla a inicialização de aplicativos de todas as unidades removíveis conectadas ao computador protegido.
   - **Confiável pelo SO**. A regra controla a inicialização de aplicativos confiáveis no sistema operacional.

   A exclusão será exibida na lista.

6. Caso seja necessário, execute as etapas 4 a 5 das instruções para cada uma das condições de acionamento da regra subsequente.

7. Caso seja necessário, edite as condições de acionamento da regra clicando no botão **Editar**.

8. Salvar alterações.

Adição de exclusões a partir de um escopo de regra de Controle de Inicialização de Aplicativos

Como adicionar exclusões do escopo da regra de Controle de Inicialização de Aplicativos no Console de Administração do Kaspersky Security Center

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

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

   b. Selecione o grupo de administração para o qual você deseja configurar a tarefa.

   c. Selecione a guia **Políticas**.

   d. Clique duas vezes no nome da política que você quer configurar.

   e. Na janela de propriedades da política, acesse a seção **Controle de atividades locais**.

   f. No bloco **Controle de Inicialização de Aplicativos**, clique no botão **Configurações**.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

2. Selecione a guia **Regras**.

3. Execute uma das seguintes ações:

   a. Clique no botão **Adicionar** caso esteja adicionando uma nova regra de Controle de Inicialização de Aplicativos.

   b. Na lista de regras de Controle de Inicialização de Aplicativos, selecione a regra para a qual deseja adicionar as exclusões e clique no botão **Editar**.

   A janela **Controle de Inicialização de Aplicativos** é aberta.

4. Na guia **Exclusões**, no menu de contexto do botão **Adicionar**, selecione um critério para criar uma exclusão do escopo da regra de Controle de Inicialização de Aplicativos:

   - **Informações do arquivo**. As informações do arquivo selecionado serão usadas como critério.

     a. Clique no botão **Procurar** na subseção **Informações do arquivo**.

     A janela padrão do Microsoft Windows **Open File** é exibida.

     b. Selecione o arquivo.

     c. Clique em **Abrir**.

     As informações sobre o arquivo selecionado serão exibidas na janela **Informações do arquivo**.

d. Selecione pelo menos uma opção:

- **Detalhes do certificado**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos assinados com um certificado digital que tenha os dados especificados.
- **Metadados**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham os metadados especificados.
- **Hash do arquivo**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham o hash SHA256 especificado.
- **Caminho do arquivo**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos no caminho especificado.

e. Caso seja necessário, no campo **Linha de comando**, insira o comando para iniciar o aplicativo na linha de comando. A regra não controla a inicialização desse aplicativo. É possível usar os caracteres ? e * para inserir uma máscara.

> O Kaspersky Embedded Systems Security não reconhece caminhos que contêm barras ("/"). Use o caractere de barra invertida ("\") nos caminhos.

f. Clique **OK**.

- **Tipo de unidade**. A regra não controla a inicialização de aplicativos de todas as unidades removíveis conectadas ao computador protegido.
- **Categoria KL**. A regra não controla a inicialização de aplicativos pertencentes às categorias KL selecionadas.
- **Confiável pela KSN**. A regra não controla a inicialização de aplicativos confiáveis na KSN.
- **Não confiável pela KSN**. A regra não controla a inicialização de aplicativos não confiáveis na KSN.
- **Confiável pelo SO**. A regra não controla a inicialização de aplicativos confiáveis no sistema operacional.

A exclusão adicionada será exibida na lista.

5. Se necessário, execute a etapa anterior das instruções para adicionar cada exclusão no escopo da regra de Controle de Inicialização de Aplicativos.
6. Caso seja necessário, edite as exclusões com um clique no botão **Editar**.
7. Salvar alterações.

Como adicionar exclusões do escopo da regra de Controle de Inicialização de Aplicativos no Kaspersky Embedded Systems Security Console

1. Na árvore do Console do Aplicativo, selecione o node **Controle do Computador** → **Controle de Inicialização de Aplicativos**.
2. Clique no link **Propriedades** no painel de resultados.

   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.
3. Selecione a guia **Regras**.
4. Execute uma das seguintes ações:

   a. Clique no botão **Adicionar** caso esteja adicionando uma nova regra de Controle de Inicialização de Aplicativos.

   b. Na lista de regras de Controle de Inicialização de Aplicativos, selecione a regra para a qual deseja adicionar as exclusões e clique no botão **Editar**.

   A janela **Controle de Inicialização de Aplicativos** é aberta.
5. Na guia **Exclusões**, no menu de contexto do botão **Adicionar**, selecione um critério para criar uma exclusão do escopo da regra de Controle de Inicialização de Aplicativos:

   - **Informações do arquivo**. As informações do arquivo selecionado serão usadas como critério.

     a. Clique no botão **Procurar** na subseção **Informações do arquivo**.

     A janela padrão do Microsoft Windows **Open File** é exibida.

     b. Selecione o arquivo.

     c. Clique em **Abrir**.

     As informações sobre o arquivo selecionado serão exibidas na janela **Informações do arquivo**.

     d. Selecione pelo menos uma opção:

     - **Detalhes do certificado**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos assinados com um certificado digital que tenha os dados especificados.
     - **Metadados**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham os metadados especificados.
     - **Hash do arquivo**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham o hash SHA256 especificado.
     - **Caminho do arquivo**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos no caminho especificado.

e. Caso seja necessário, no campo **Linha de comando**, insira o comando para iniciar o aplicativo na linha de comando. A regra não controla a inicialização desse aplicativo. É possível usar os caracteres ? e * para inserir uma máscara.

> O Kaspersky Embedded Systems Security não reconhece caminhos que contêm barras ("/"). Use o caractere de barra invertida ("\") nos caminhos.

f. Clique **OK**.

- **Tipo de unidade**. A regra não controla a inicialização de aplicativos de todas as unidades removíveis conectadas ao computador protegido.
- **Categoria KL**. A regra não controla a inicialização de aplicativos pertencentes às categorias KL selecionadas.
- **Confiável pela KSN**. A regra não controla a inicialização de aplicativos confiáveis na KSN.
- **Não confiável pela KSN**. A regra não controla a inicialização de aplicativos não confiáveis na KSN.
- **Confiável pelo SO**. A regra não controla a inicialização de aplicativos confiáveis no sistema operacional.

A exclusão adicionada será exibida na lista.

6. Se necessário, execute a etapa anterior das instruções para adicionar cada exclusão no escopo da regra de Controle de Inicialização de Aplicativos.
7. Caso seja necessário, edite as exclusões com um clique no botão **Editar**.
8. Salvar alterações.

Como adicionar exclusões do escopo da regra de Controle de Inicialização de Aplicativos no Kaspersky Security Center Web Console

1. Vá para as configurações de Controle de Dispositivos na política que deseja configurar.

   a. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

   b. Clique no nome da política do Kaspersky Embedded Systems Security.
   A janela de propriedades da política é exibida.

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

   d. Selecione a seção **Controle de atividades locais**.

   e. No bloco **Controle de Inicialização de Aplicativos**, clique no botão **Configurar**.
   A janela **Controle de Inicialização de Aplicativos** é exibida na guia **Geral**.

2. Selecione a guia **Regras**.

3. Clique **Adicionar**.

   A janela **Configurações de regra** é aberta.

4. Na guia **Exclusões**, clique no botão **Adicionar**.

   A janela **Configurações de regra** é aberta.

5. Selecione um critério para criar uma exclusão no escopo da regra de Controle de Inicialização de Aplicativos:

   - **Informações do arquivo**. A regra não controla a inicialização de aplicativos cujos dados correspondem aos dados no arquivo.

     a. Em **Critérios de acionamento de regras**, especifique o valor para pelo menos um critério:

     - **Certificado digital**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos assinados com um certificado digital que tenha os dados especificados.
     - **Metadados**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham os metadados especificados.
     - **Hash SHA256**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos que tenham o hash SHA256 especificado.
     - **Caminho do arquivo**. Caso essa caixa de seleção esteja marcada, a regra não controlará a inicialização de aplicativos no caminho especificado.

     b. Clique **OK**.

   - **Categoria KL**. A regra não controla a inicialização de aplicativos pertencentes às categorias KL selecionadas.
   - **Tipo de unidade**. A regra não controla a inicialização de aplicativos de todas as unidades removíveis conectadas ao computador protegido.
   - **Confiável pelo SO**. A regra não controla a inicialização de aplicativos confiáveis no sistema operacional.

   A exclusão será exibida na lista.

6. Se necessário, execute as etapas 4 a 5 das instruções para adicionar cada exclusão subsequente do escopo da regra de Controle de Inicialização de Aplicativos.

7. Caso seja necessário, edite as exclusões com um clique no botão **Editar**.

8. Salvar alterações.

Ativar o modo de Permissão padrão

É possível permitir a inicialização de todos os aplicativos por meio das regras de permissão do Controle de Inicialização de Aplicativos especialmente configuradas.

Para permitir a inicialização de todos os aplicativos:

1. Adicione manualmente duas regras de permissão do Controle de Inicialização de Aplicativos com os seguintes parâmetros:
   - Tipo de regra: *Permitir*, Escopo: *Arquivos executáveis*, Caminho do arquivo: `?:\`.
   - Tipo de regra: *Permitir*, Escopo: *Pacotes de scripts e MSI*, Caminho do arquivo: `?:\`.
2. Caso as regras de negação do Controle de Inicialização de Aplicativos tenham sido adicionadas, exclua essas regras.
3. Para todas as regras de permissão do Controle de Inicialização de Aplicativos criadas anteriormente, exclua as exclusões.
4. Salvar alterações.

Gerando um arquivo TXT com uma seleção de eventos de aplicativo bloqueado pelo Kaspersky Security Center

É possível exportar uma seleção de eventos de aplicativos bloqueados pelo Kaspersky Security Center para um arquivo TXT e, em seguida, importar esses dados para gerar uma lista de regras permitidas do Controle de Inicialização de Aplicativos em uma política que estiver configurando.

Como gerar um arquivo TXT com uma seleção de eventos de aplicativos bloqueados pelo Kaspersky Security Center usando o Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados**.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela de propriedades da política, acesse a seção **Registros e notificações**.
6. No bloco **Logs de tarefas**, clique no botão **Configurações**.

   A janela **Notificações** é aberta.
7. Expanda o nó **Controle de atividades locais**.
8. Selecione a seção **Controle de Inicialização de Aplicativos**.
9. Na lista de eventos do Controle de Inicialização de Aplicativos, na coluna **Enviar eventos ao Kaspersky Security Center**, marque as caixas de seleção ao lado de *Proibida a inicialização do aplicativo* e *Proibida a inicialização do aplicativo em modo de teste*.
10. Salvar alterações.

11. Na seção **Configuração de eventos** da política, verifique e confirme se o tempo de duração do armazenamento do evento especificado no campo **Armazenar no banco de dados do Servidor de Administração por (dias)** é maior que o período para o qual se planeja coletar as informações sobre as inicializações impedidas de aplicativos (o padrão é 30 dias).

    Depois que o período de retenção do log de Controle de Dispositivos expirar, os eventos registrados serão excluídos e não aparecerão no relatório.

12. Ativar a política configurada para coletar dados referentes a inicializações negadas de aplicativos.
13. Se necessário, modifique o modo do Controle de Dispositivos.
14. Quando o período de coleta de informações sobre as inicializações impedidas de aplicativos expirar, faça selecione eventos em *Proibida a inicialização do aplicativo* e *Proibida a inicialização do aplicativo em modo de teste* e exporte para um arquivo TXT. Para saber mais detalhes, consulte a seção "Seleções de eventos" na *Ajuda do Kaspersky Security Center*.
15. Abra o arquivo TXT exportado.
16. Caso seja necessário, edite a lista de eventos.

Como gerar um arquivo TXT com uma seleção de eventos de aplicativos bloqueados pelo Kaspersky Security Center usando o Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

    A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Logs e notificações**.
5. No bloco **Logs de tarefas**, clique no botão **Configurar**.

    A janela **Logs de tarefas** é aberta.
6. Selecione a seção **Controle de Inicialização de Aplicativos**.
7. Na lista de eventos do Controle de Inicialização de Aplicativos, na coluna **Enviar eventos ao Kaspersky Security Center**, marque as caixas de seleção ao lado de *Proibida a inicialização do aplicativo* e *Proibida a inicialização do aplicativo em modo de teste*.
8. Salvar alterações.

9. Na guia **Configuração de eventos** da política que estiver sendo configurada, verifique e confirme se o tempo de duração do armazenamento do evento especificado no campo **Armazenar no banco de dados do Servidor de Administração por (dias)** é maior que o período para o qual se planeja coletar as informações sobre as inicializações impedidas de aplicativos (o padrão é 30 dias).

   Depois que o período de retenção do log de Controle de Dispositivos expirar, os eventos registrados serão excluídos e não aparecerão no relatório.

10. Ativar a política configurada para coletar dados referentes a inicializações negadas de aplicativos.
11. Se necessário, modifique o modo do Controle de Dispositivos.
12. Quando o período de coleta de informações sobre as inicializações impedidas de aplicativos expirar, faça selecione eventos em *Proibida a inicialização do aplicativo* e *Proibida a inicialização do aplicativo em modo de teste* e exporte para um arquivo TXT. Para saber mais detalhes, consulte a seção "Seleções de eventos" na *Ajuda do Kaspersky Security Center*.
13. Abra o arquivo TXT exportado.
14. Caso seja necessário, edite a lista de eventos.

Configuração de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

Como configurar a tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos no Console de Administração do Kaspersky Security Center

1. Abra as propriedades da tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos.

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

   b. Selecione o grupo de administração para o qual você deseja configurar a tarefa.

   c. Selecione a guia **Tarefas**.

   d. Na lista de tarefas de grupo, abra a tarefa Gerador de Regras de Controle de Inicialização de Aplicativos com um clique duplo no nome da tarefa.

   A janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos** é aberta.

2. Ir para a seção **Opções**.
3. Caso seja necessário, insira o prefixo para nomes de regras na guia **Regras**.

4. Em **Escopo de uso da regra de permissão**, especifique o método que deseja usar para criar as regras de permissão:

   - Criar regras de permissão com base nos aplicativos em execução.
   - Criar regras de permissão para aplicativos das pastas.

5. Na guia **Configurações**, selecione o critério pelo qual a tarefa será aplicada durante a criação de regras de permissão do Controle de Inicialização de Aplicativos:

   - Usar certificado digital.
   - Usar o assunto e a impressão digital do certificado digital.
   - Se o certificado estiver ausente, usar.
   - Usar hash SHA256.

6. Defina a configuração **Adicionar um caminho do arquivo para as regras geradas de acordo com as somas de hash**.

   Caso esta caixa de seleção esteja marcada, ao exportar regras, o Kaspersky Embedded Systems Security adicionará caminhos completos para arquivos executáveis ao arquivo XML. Os caminhos completos podem ajudar a saber a qual software um arquivo executável pertence.

   Caso a caixa de seleção esteja desmarcada, o arquivo XML conterá apenas nomes e hashes SHA256 de arquivos executáveis. Por padrão, a caixa de seleção fica desmarcada.

7. Adicionar os usuários e/ou grupos de usuários que possam iniciar aplicativos que satisfaçam as regras criadas usando a tarefa.

   a. No menu de contexto do botão **Adicionar**, selecione o método para adicionar usuários ou grupos.

   b. O procedimento abre uma janela; nessa janela, digite ou selecione o nome de um usuário ou grupo de usuários.

   c. Clique **OK**.

   d. Conclua as etapas de a até c para cada usuário ou grupo de usuários.

8. 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**. É possível clicar no botão **Procurar** para especificar um caminho para o qual o Kaspersky Embedded Systems Security exportará as regras de permissão em um arquivo XML quando a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos for concluída.
   - Adicionar os detalhes sobre o dispositivo protegido ao nome do arquivo.

9. Caso seja necessário, especifique os objetos que deseja excluir do escopo da tarefa na guia **Exclusões**.

10. Clique no botão **OK** na janela **Propriedades:Gerador de Regras de Controle de Inicialização de Aplicativos**.

Como configurar a tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Tarefas**.

2. Na lista de tarefas de grupo, abra a tarefa Gerador de Regras de Controle de Inicialização de Aplicativos.

   A janela **Gerador de Regras de Controle de Inicialização de Aplicativos** é aberta.

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

4. Caso seja necessário, insira um prefixo para os nomes das regras na seção **Escopo de uso da regra de permissão**.

5. Em **Escopo de uso da regra de permissão**, especifique o método que deseja usar para criar as regras de permissão:

   - Criar regras de permissão com base nos aplicativos em execução
   - Criar regras de permissão para aplicativos das pastas

6. Na guia **Parâmetros**, selecione o critério pelo qual a tarefa será aplicada durante a criação de regras de permissão do Controle de Inicialização de Aplicativos:

   - Usar certificado digital.
   - Usar o assunto e a impressão digital do certificado digital.
   - Se o certificado estiver ausente, use.
   - Usar hash SHA256.

7. Defina a configuração **Adicionar um caminho do arquivo para as regras geradas de acordo com as somas de hash**.

   Caso esta caixa de seleção esteja marcada, ao exportar regras, o Kaspersky Embedded Systems Security adicionará caminhos completos para arquivos executáveis ao arquivo XML. Os caminhos completos podem ajudar a saber a qual software um arquivo executável pertence.

   Caso a caixa de seleção esteja desmarcada, o arquivo XML conterá apenas nomes e hashes SHA256 de arquivos executáveis. Por padrão, a caixa de seleção fica desmarcada.

8. Adicionar os usuários e/ou grupos de usuários que possam iniciar aplicativos que satisfaçam as regras criadas usando a tarefa.

   a. Clique **Selecionar usuário ou grupo**.

   b. O procedimento abre uma janela; nessa janela, digite ou selecione o nome de um usuário ou grupo de usuários.

c. Clique **Selecionar**.

d. Conclua as etapas de a até c para cada usuário ou grupo de usuários.

9. 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.
   - **As regras de permissão serão exportadas para um arquivo**. No campo **Especifique o caminho completo para um arquivo com extensão .xml**, é possível especificar um caminho para o qual o Kaspersky Embedded Systems Security exportará as regras de permissão para um arquivo XML quando a tarefa Gerador de Regras de Controle de Inicialização de Aplicativos for concluída.
   - Adicionar os detalhes sobre o dispositivo protegido ao nome do arquivo.

10. Caso seja necessário, especifique os objetos que deseja excluir do escopo da tarefa na guia **Exclusões**.

11. Clique no botão **OK** na subseção **Gerador de Regras de Controle de Inicialização de Aplicativos**.

Usando uma tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos.

Para criar regras com o uso de uma tarefa de grupo Gerador de Regras de Controle de Inicialização de Aplicativos:

1. Crie uma tarefa de grupo *Gerador de Regras de Controle de Inicialização de Aplicativos* ou selecione uma tarefa existente.
2. Configure a tarefa Gerador de Regras de Controle de Inicialização de Aplicativos.
3. Execute a tarefa Gerador de Regras de Controle de Inicialização de Aplicativos.

Após a conclusão da tarefa, de acordo com suas configurações:

- Caso tenha especificado a ação **Adicionar regras de permissão à lista de regras de Controle de Inicialização de Aplicativos** durante a conclusão da tarefa, as regras geradas do Controle de Inicialização de Aplicativos serão adicionadas à lista de configurações do Controle de Inicialização de Aplicativos no Console do Aplicativo.
- Caso tenha especificado a ação **As regras de permissão serão exportadas para um arquivo** durante a conclusão da tarefa, as regras geradas do Controle de Inicialização de Aplicativos serão salvas em um arquivo XML no caminho especificado nas configurações da tarefa.

As listas contêm regras de permissão para inicialização de aplicativos cujo tipo corresponde às configurações da tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos.

Controle de Dispositivos

O Controle de Dispositivos gerencia o acesso de usuário a dispositivos que estão instalados ou conectados no computador (por exemplo, discos rígidos, câmeras ou módulos Wi-Fi). Com isso, você pode proteger o computador de infecções quando esse tipo de dispositivo é conectado e evitar perda ou vazamento de dados.

O controle de dispositivos oferece a seguinte funcionalidade:

- Gerenciamento de permissões de acesso do usuário nos dispositivos de armazenamento (por exemplo, unidades removíveis, telefones celulares, unidades de CD/DVD, etc.).
- Controle da conexão de dispositivos sem um sistema de arquivos (por exemplo, modems externos, adaptadores Bluetooth, teclados USB, etc.).
- Gerenciamento de conexões Wi-Fi.

Por padrão, o Controle de Dispositivos está desativado. Quando o Controle de Dispositivos é ativado, por padrão, o Kaspersky Embedded Systems Security nega o acesso aos seguintes tipos de dispositivos:

- Unidades removíveis (inclusive unidades flash USB)
- Disquetes
- Unidades de CD/DVD-ROM
- Dispositivos portáteis (MTP)
- Modems.
- Leitores de cartões inteligentes
- Adaptadores de rede externos
- Bluetooth (exceto dispositivos de entrada)

Níveis do controle de dispositivos

O Kaspersky Embedded Systems Security controla o acesso ao dispositivo nos seguintes níveis:

1. **Tipo de dispositivo**.

   Ao conectar um dispositivo ao computador, o sistema operacional determina o tipo de dispositivo: impressora, unidade removível, unidade de CD/DVD etc. Neste nível, é possível permitir ou negar a conexão de dispositivos por tipo.

2. **Barramento de conexão**.

   O *barramento de conexão* é uma interface usada para conectar dispositivos ao computador. Alguns tipos de dispositivos têm várias interfaces de conexão. Por exemplo, é possível conectar uma impressora na porta USB ou na porta serial (COM).

   Nesse nível, é possível permitir ou negar o acesso aos dispositivos, dependendo do barramento de conexão.

Por exemplo, suponha que o acesso via USB tenha sido negado. O Kaspersky Embedded Systems Security nega o acesso a todos os tipos de dispositivos com o modo **Depende do barramento de conexão** quando conectado via USB.

> Caso o modo de acesso **Permitir** ou **Bloquear** seja selecionado para o dispositivo, o controle de acesso desconsidera o barramento de conexão do dispositivo.

3. **Dispositivos confiáveis**.

   Dispositivos confiáveis aqueles aos quais os usuários especificados têm acesso total a qualquer momento.

Modos de operação do controle de dispositivos

O controle de dispositivos pode funcionar nos seguintes modos:

- **Modo ativo**.

  O Kaspersky Embedded Systems Security nega ou permite os dispositivos de acordo com as regras de acesso do dispositivo configuradas. O aplicativo também permite o acesso aos dispositivos confiáveis. O aplicativo registra os eventos de conexão e desconexão do dispositivo.

- **Informar**.

  O Kaspersky Embedded Systems Security permite todos os dispositivos e registra os logs correspondentes. Todos os dispositivos são permitidos. Este modo está definido por padrão. É possível ativar esse modo para fazer uma auditoria dos dispositivos em sua organização e usar essas informações para elaborar uma lista de dispositivos confiáveis.

Regras de acesso do dispositivo

Uma *regra de acesso do dispositivo* é um conjunto de configurações que determina de que forma os usuários podem acessar dispositivos que estão instalados ou conectados em um computador. Essas configurações incluem acesso a um dispositivo específico, um agendamento de acesso e permissões de leitura ou gravação. O grupo de configurações para uma regra de acesso muda dependendo do tipo de dispositivo (veja a tabela abaixo).

Configurações da regra de acesso

Dispositivos	Atribuição de usuários e/ou grupos de usuários	Agendamento para acesso a dispositivos	Permissão para leitura/gravação	Monitoramento do barramento de conexão
Discos rígidos	✓	✓	✓	✓
Unidades removíveis (inclusive unidades flash USB)	✓	✓	✓	✓
Disquetes	✓	✓	✓	✓
Unidades de CD/DVD-ROM	✓	✓	✓	✓
Dispositivos portáteis (MTP)	✓	✓	✓	✓
Impressoras locais	✓	–	–	✓
Impressoras de rede	✓	–	–	–
Modems	–	–	–	✓
Streamers	–	–	–	✓
Dispositivos multifuncionais	–	–	–	✓

Dispositivos	Atribuição de usuários e/ou grupos de usuários	Agendamento para acesso a dispositivos	Permissão para leitura/gravação	Monitoramento do barramento de conexão
Leitores de cartões inteligentes	–	–	–	✓
Dispositivos do Windows CE USB ActiveSync	–	–	–	✓
Adaptadores de rede externos	–	–	–	✓
Bluetooth	–	–	–	–
Câmeras e scanners	–	–	–	✓
Wi-Fi	–	–	–	–
Teclados USB	–	–	–	✓
Mouses USB	–	–	–	✓

Controle de acesso de dispositivos por tipo

O controle de dispositivos permite controlar o acesso aos dispositivos por tipo do dispositivo. O tipo de um dispositivo é determinado pelo sistema operacional quando o dispositivo é conectado. É possível descobrir o tipo do dispositivo por meio da ferramenta Gerenciador de dispositivos integrada ao sistema operacional. Para gerenciar o acesso ao dispositivo gerenciado, será necessário configurar as regras. Uma *regra de acesso do dispositivo* é um conjunto de configurações que determina de que forma os usuários podem acessar dispositivos que estão instalados ou conectados em um computador. Essas configurações incluem acesso a um dispositivo específico, um agendamento de acesso e permissões de leitura ou gravação. O grupo de configurações para uma regra de acesso muda dependendo do tipo de dispositivo (veja a tabela abaixo).

Você pode configurar o acesso do dispositivo da seguinte forma:

- **Permitir**.

  O Kaspersky Embedded Systems Security concede acesso total aos dispositivos para todos os usuários.

- **Bloquear**.

  O Kaspersky Embedded Systems Security bloqueia a conexão do dispositivo. O aplicativo permite conectar apenas os dispositivos confiáveis.

- **Depende do barramento de conexão**.

  O Kaspersky Embedded Systems Security identifica o barramento de conexão do dispositivo e executa o controle de acesso de acordo com o modo de acesso do barramento de conexão. O aplicativo também permite conectar dispositivos confiáveis.

- **Por regras**.

  Para alguns tipos de dispositivos, é possível selecionar usuários ou um grupo de usuários que terão permissão para usar dispositivos, configurar uma programação de acesso a dispositivos e permissões de leitura e gravação. O aplicativo também permite conectar dispositivos confiáveis.

Tenha cuidado ao configurar o acesso a dispositivos do tipo **Discos rígidos**. Caso o acesso à unidade do sistema seja proibido, o aplicativo poderá travar o sistema operacional de inicialização (BSOD).

Caso um dispositivo esteja fora do esquema de classificação do controle de dispositivos, o acesso a tal dispositivo não poderá ser restrito.

Como controlar o acesso a dispositivos por tipo no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controle de atividades locais**.
4. Na seção **Controle de dispositivos**, clique no botão **Configurações**.
5. Marque a caixa de seleção **Controle de dispositivos**.
6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.
7. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A guia **Tipos de dispositivos** exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente Controle de Dispositivos.
8. Configurar regras de acesso para dispositivos móveis

   a. Selecione um modo de acesso: **Permitir**, **Bloquear**, **Depende do barramento de conexão**, **Por regras**.

   Para selecionar o modo de acesso **Por regras**, será necessário dar um duplo clique para abrir o acesso às propriedades da regra.

   b. Caso o modo de acesso **Depende do barramento de conexão** seja selecionado, será necessário configurar as regras de acesso para as interfaces de conexão na guia **Barramentos de conexão**.

   c. Para os dispositivos de armazenamento (por exemplo, dispositivos removíveis), é possível configurar os direitos de acesso de usuários individuais. Também é possível configurar um agendamento de acesso ao dispositivo e configurar as permissões de leitura e gravação.

   d. Caso seja necessário, configurar as regras de impressão.

   e. Caso seja necessário, configurar as regras de conexão Wi-Fi.
9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como controlar o acesso a dispositivos por tipo no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controle de atividades locais** → **Controle de dispositivos** e clique no botão **Configurar**.

   A janela **Controle de dispositivos** é aberta.
5. Marque a caixa de seleção **Ativar o Controle de dispositivos**.

6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.

7. No bloco **Configurações do Controle de dispositivos**, clique em **Regras de acesso para dispositivos e redes Wi-Fi**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.

8. Configurar regras de acesso para dispositivos móveis

   a. Selecione um modo de acesso: **Permitir**, **Bloquear**, **Depende do barramento de conexão**, **Por regras**.

      Caso o modo de acesso não esteja disponível no menu suspenso, abra as propriedades da regra de acesso com um clique duplo no tipo do dispositivo.

   b. Caso o modo de acesso **Depende do barramento de conexão** seja selecionado, será necessário voltar à janela com as configurações gerais do controle de dispositivos, clicar em **Barramentos de conexão** e configurar as regras de acesso para as interfaces de conexão.

   c. Para os dispositivos de armazenamento (por exemplo, dispositivos removíveis), é possível configurar os direitos de acesso de usuários individuais. Também é possível configurar um agendamento de acesso ao dispositivo e configurar as permissões de leitura e gravação.

   d. Caso seja necessário, configurar as regras de impressão.

   e. Caso seja necessário, configurar as regras de conexão Wi-Fi.

9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como controlar o acesso a dispositivos por tipo no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador → Controle de dispositivos**.

2. no painel de resultados do node **Controle de dispositivos**, clique no link **Propriedades**.

   A janela **Propriedades: Controle de dispositivos** é aberta.

3. Marque a caixa de seleção **Controle de dispositivos**.

4. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.

5. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.

6. Configurar regras de acesso para dispositivos móveis

   a. Selecione o modo de acesso: **Permitir**, **Bloquear**, **Depende do barramento de conexão**, **Por regras**.

      Para selecionar o modo de acesso **Por regras**, será necessário dar um duplo clique para abrir o acesso às propriedades da regra.

   b. Caso o modo de acesso **Depende do barramento de conexão** seja selecionado, será necessário configurar regras de acesso para as interfaces de conexão na guia **Barramentos de conexão**.

c. Para os dispositivos de armazenamento (por exemplo, dispositivos removíveis), é possível configurar os direitos de acesso de usuários individuais. Também é possível configurar um agendamento de acesso ao dispositivo e configurar as permissões de leitura e gravação.

d. Caso seja necessário, configurar as regras de impressão.

e. Caso seja necessário, configurar as regras de conexão Wi-Fi.

7. Salvar alterações.

Assim, quando o usuário tentar obter acesso ao dispositivo, o aplicativo bloqueará o acesso de acordo com as regras. O Kaspersky Embedded Systems Security também registra os logs do evento correspondente. Caso queira conceder acesso a dispositivos individuais, é possível adicionar esses dispositivos à lista de dispositivos confiáveis.

Controle de conexões Wi-Fi

O controle de dispositivos permite gerenciar a conexão Wi-Fi do computador (terminal). As redes Wi-Fi públicas podem ser inseguras e seu uso pode resultar em perda de dados. O Controle de Dispositivos permite bloquear a conexão de um usuário ao Wi-Fi ou permite a conexão apenas a redes confiáveis. Por exemplo, é possível permitir a conexão apenas à rede Wi-Fi corporativa suficientemente segura. O Controle de Dispositivos bloqueará o acesso a todas as redes Wi-Fi, exceto aquelas especificadas na lista confiável.

Em computadores que executam o Windows 11, é necessário ativar Serviços de localização para controlar conexões Wi-Fi. Para fazer isso, basta ativar o comutador **Serviços de localização** nas configurações do sistema operacional (**Configurações** → **Privacidade e segurança** → **Localização**). Se os Serviços de localização estiverem desativados, o Kaspersky Embedded Systems Security não controlará conexões com as redes Wi-Fi.

Como restringir as conexões Wi-Fi no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controle de atividades locais**.
4. Na seção **Controle de dispositivos**, clique no botão **Configurações**.
5. Marque a caixa de seleção **Controle de dispositivos**.
6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.
7. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A guia **Tipos de dispositivos** exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente Controle de Dispositivos.

8. Para os dispositivos **Wi-Fi**, configure uma regra de acesso:

    a. Selecione um modo de acesso: **Permitir**, **Bloquear**, **Bloquear com exceções**.

    b. Caso o modo **Bloquear com exceções** seja selecionado, será necessário criar uma lista de redes Wi-Fi confiáveis:

        1. Clique duas vezes no tipo de dispositivo **Wi-Fi** para abrir a lista de redes Wi-Fi confiáveis.

        2. Clique no botão **Adicionar** na janela que se abre.

        3. Isso abre uma janela; nessa janela, configure a rede Wi-Fi confiável (veja a figura abaixo):

            - **Nome da rede**. Nome ou SSID (Service Set Identifier) da rede Wi-Fi.
            - **Tipo de autenticação**. Tipo de autenticação usado ao conectar a redes Wi-Fi.
            - **Tipo de criptografia**. Tipo de criptografia usado para proteger o tráfego Wi-Fi.
            - **Comentário**. Mais informações sobre a rede Wi-Fi adicionada.

    É possível visualizar as configurações da rede Wi-Fi confiável nas configurações do roteador.

    > Uma rede Wi-Fi será considerada confiável se as suas configurações coincidirem com todas as configurações especificadas na regra.

9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como restringir as conexões Wi-Fi no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controle de atividades locais** → **Controle de dispositivos** e clique no botão **Configurar**.

   A janela **Controle de dispositivos** é aberta.
5. Marque a caixa de seleção **Ativar o Controle de dispositivos**.
6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.
7. No bloco **Configurações do Controle de dispositivos**, clique em **Regras de acesso para dispositivos e redes Wi-Fi**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.
8. Clique duas vezes no tipo de dispositivo **Wi-Fi** para abrir as propriedades da regra de acesso.

9. Selecione um modo de acesso: **Permitir**, **Bloquear**, **Bloquear com exceções**.

10. Caso o modo **Bloquear com exceções** seja selecionado, será necessário criar uma lista de redes Wi-Fi confiáveis:

    1. No bloco **Redes Wi-Fi confiáveis**, clique no botão **Adicionar**.

    2. Isso abre uma janela; nessa janela, configure a rede Wi-Fi confiável (veja a figura abaixo):

       - **Nome da rede**. Nome ou SSID (Service Set Identifier) da rede Wi-Fi.
       - **Tipo de autenticação**. Tipo de autenticação usado ao conectar a redes Wi-Fi.
       - **Tipo de criptografia**. Tipo de criptografia usado para proteger o tráfego Wi-Fi.
       - **Comentário**. Mais informações sobre a rede Wi-Fi adicionada.

    É possível visualizar as configurações da rede Wi-Fi confiável nas configurações do roteador.

    > Uma rede Wi-Fi será considerada confiável se as suas configurações coincidirem com todas as configurações especificadas na regra.

11. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como restringir conexões Wi-Fi no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Controle de dispositivos**.

2. no painel de resultados do node **Controle de dispositivos**, clique no link **Propriedades**.

   A janela **Propriedades: Controle de dispositivos** é aberta.

3. Marque a caixa de seleção **Controle de dispositivos**.

4. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.

5. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.

6. Para dispositivos **Wi-Fi**, configure uma regra de acesso:

   a. Selecione um modo de acesso: **Permitir**, **Bloquear**, **Bloquear com exceções**.

   b. Caso o modo **Bloquear com exceções** seja selecionado, será necessário criar uma lista de redes Wi-Fi confiáveis:

      1. Clique duas vezes no tipo de dispositivo **Wi-Fi** para abrir a lista de redes Wi-Fi confiáveis.

      2. Clique no botão **Adicionar** na janela que se abre.

3. Isso abre uma janela; nessa janela, configure a rede Wi-Fi confiável (veja a figura abaixo):

- **Nome da rede**. Nome ou SSID (Service Set Identifier) da rede Wi-Fi.
- **Tipo de autenticação**. Tipo de autenticação usado ao conectar a redes Wi-Fi.
- **Tipo de criptografia**. Tipo de criptografia usado para proteger o tráfego Wi-Fi.
- **Comentário**. Mais informações sobre a rede Wi-Fi adicionada.

É possível visualizar as configurações da rede Wi-Fi confiável nas configurações do roteador.

> Uma rede Wi-Fi será considerada confiável se as suas configurações coincidirem com todas as configurações especificadas na regra.

7. Salvar alterações.

Assim, quando um usuário tenta se conectar a uma rede Wi-Fi não listada como confiável, o aplicativo bloqueia a conexão.

Controle de impressão

O controle de dispositivos permite configurar o acesso do usuário a impressoras locais e de rede.

Controle de impressoras locais

O Kaspersky Embedded Systems Security controla a conexão com a impressora local através dos seguintes barramentos: USB, Porta serial (COM), Porta paralela (LPT).

> O Kaspersky Embedded Systems Security controla a conexão de impressoras locais a portas COM e LPT somente no nível do barramento. Ou seja, para impedir a conexão de impressoras a portas COM e LPT, para o tipo de dispositivo **Impressoras locais**, selecione o modo **Depende do barramento de conexão** e proíba a conexão de dispositivos a barramentos COM e LPT.

Para impressoras conectadas via USB, o aplicativo exerce controle em dois níveis: tipo de dispositivo (impressoras locais) e barramento de conexão (USB).

É possível selecionar um dos seguintes modos de acesso às impressoras locais via USB:

- **Permitir**. O Kaspersky Embedded Systems Security concede acesso total a impressoras locais a todos os usuários. Os usuários podem conectar impressoras e imprimir documentos com o uso dos meios que o sistema operacional oferece.
- **Bloquear**. O Kaspersky Embedded Systems Security bloqueia a conexão de impressoras locais. O aplicativo permite conectar apenas as impressoras confiáveis.

- **Depende do barramento de conexão**. O Kaspersky Embedded Systems Security permite a conexão a impressoras locais de acordo com o status da conexão de barramento USB (**Permitir** ou **Bloquear**).
- **Por regras**. Para controlar a impressão, é necessário adicionar *regras de impressão*. Nas regras, é possível selecionar os usuários ou um grupo de usuários para os quais se deseja permitir ou bloquear o acesso à impressão de documentos em impressoras locais.

Controle de impressoras de rede

O Kaspersky Embedded Systems Security permite configurar o acesso à impressão em impressoras de rede. É possível selecionar um dos seguintes modos de acesso às impressoras de rede:

- **Permitir e não registrar** . O Kaspersky Embedded Systems Security não controla a impressão em impressoras de rede. O aplicativo concede acesso à impressão para todos os usuários e não salva as informações sobre a impressão no log de eventos.
- **Permitir**. O Kaspersky Embedded Systems Security concede acesso à impressão em impressoras de rede a todos os usuários.
- **Bloquear**. O Kaspersky Embedded Systems Security restringe o acesso a impressoras de rede para todos os usuários. O aplicativo permite o acesso apenas a impressoras confiáveis.
- **Por regras**. Para controlar a impressão, é necessário adicionar *regras de impressão*. Nas regras, é possível selecionar os usuários ou um grupo de usuários para os quais se deseja permitir ou bloquear o acesso à impressão de documentos em impressoras de rede.

Adicionar regras de impressão para impressoras

Como adicionar regras de impressoras no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controle de atividades locais**.
4. Na seção **Controle de dispositivos**, clique no botão **Configurações**.
5. Marque a caixa de seleção **Controle de dispositivos**.
6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.
7. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A guia **Tipos de dispositivos** exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente Controle de Dispositivos.

8. Configurar as regras de acesso à impressora:

    a. Para os tipos dr dispositivo **Impressoras locais** e **Impressoras de rede**, configure as regras de acesso: **Permitir**, **Bloquear**, **Permitir e não registrar** (somente impressoras de rede), **Depende do barramento de conexão** (somente impressoras locais), **Por regras**.

    b. Caso o modo de acesso **Depende do barramento de conexão** seja selecionado, será necessário configurar regras de acesso para as interfaces de conexão na guia **Barramentos de conexão**.

    c. Caso o modo de acesso **Por regras** seja selecionado, será necessário configurar as regras de impressão:

        1. Clique duas vezes nos tipos de dispositivo **Impressoras locais** e **Impressoras de rede** para abrir as propriedades da regra de acesso.

        2. Selecione os usuários ou grupo de usuários para os quais deseja aplicar a regra de impressão. Para isso, clique no botão **Adicionar**.

            Uma janela será exibida para adicionar uma nova regra de impressão.

        3. Atribua uma prioridade à *entrada da regra*. Uma entrada de regra inclui os seguintes atributos: conta de usuário, ação (permitir/bloquear) e prioridade.

            Uma regra tem uma prioridade específica. Se um usuário foi adicionado a vários grupos, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Embedded Systems Security permite a atribuição de 0 a 10.000. Quanto mais alto for o valor, maior é a prioridade. Em outras palavras, uma entrada com o valor 0 possui a prioridade mais baixa.

            Por exemplo, você pode conceder permissões de somente leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para fazer isso, atribua uma prioridade de 1 para o grupo de administradores e atribua uma prioridade de 0 para o grupo Todos.

            A prioridade da regra de bloqueio é mais alta do que a de permissão. Em outras palavras, se um usuário foi adicionado a vários grupos e a prioridade de todas as regras é a mesma, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

        4. Em **Ação**, configure o acesso do usuário para imprimir na impressora.

        5. Clique em **Usuários e grupos** e selecione usuários ou grupos de usuários para acessar a impressão. É possível selecionar usuários no Active Directory, na lista de contas no Kaspersky Security Center ou ao inserir um nome de usuário local manualmente. A Kaspersky recomenda usar contas de usuário locais somente em casos especiais quando não for possível usar contas de usuário de domínio.

        6. Clique **OK**.

9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como adicionar regras de impressoras no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

    A janela de propriedades da política é exibida.

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

4. Vá para **Controle de atividades locais → Controle de dispositivos** e clique no botão **Configurar**.

   A janela **Controle de dispositivos** é aberta.

5. Marque a caixa de seleção **Ativar o Controle de dispositivos**.

6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.

7. No bloco **Configurações do Controle de dispositivos**, clique em **Regras de acesso para dispositivos e redes Wi-Fi**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.

8. Configurar as regras de acesso à impressora:

   a. Para os tipos de dispositivo **Impressoras locais** e **Impressoras de rede**, selecione um modo de acesso: **Permitir**, **Bloquear**, **Permitir e não registrar** (somente para impressoras de rede), **Depende do barramento de conexão** (somente para impressoras locais), **Por regras**.

      Caso o modo de acesso não esteja disponível no menu suspenso, abra as propriedades da regra de acesso com um clique duplo no tipo do dispositivo.

   b. Caso o modo de acesso **Depende do barramento de conexão** seja selecionado, será necessário voltar à janela com as configurações gerais do Controle de dispositivos, clicar em **Barramentos de conexão** e configurar regras de acesso para as interfaces de conexão.

   c. Caso seja necessário configurar a impressão:

      1. Clique duas vezes no tipo de dispositivo **Impressoras locais** ou **Impressoras de rede** para abrir as propriedades da regra de acesso.

      2. Selecione o modo de acesso **Por regras**.

      3. Selecione os usuários ou grupo de usuários para os quais deseja aplicar a regra de impressão. Para isso, clique no botão **Adicionar**.

         Uma janela será exibida para adicionar uma nova regra de impressão.

      4. Atribua uma prioridade à *entrada da regra*. Uma entrada de regra inclui os seguintes atributos: conta de usuário, ação (permitir/bloquear) e prioridade.

         Uma regra tem uma prioridade específica. Se um usuário foi adicionado a vários grupos, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Embedded Systems Security permite a atribuição de 0 a 10.000. Quanto mais alto for o valor, maior é a prioridade. Em outras palavras, uma entrada com o valor 0 possui a prioridade mais baixa.

         Por exemplo, você pode conceder permissões de somente leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para fazer isso, atribua uma prioridade de 1 para o grupo de administradores e atribua uma prioridade de 0 para o grupo Todos.

         A prioridade da regra de bloqueio é mais alta do que a de permissão. Em outras palavras, se um usuário foi adicionado a vários grupos e a prioridade de todas as regras é a mesma, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

      5. Em **Ação**, configure o acesso do usuário para imprimir na impressora.

6. Em **Usuários e grupos**, clique em **Adicionar** e selecione usuários ou grupos de usuários para acessar a impressão. É possível selecionar usuários no Active Directory, na lista de contas no Kaspersky Security Center ou ao inserir um nome de usuário local manualmente. A Kaspersky recomenda usar contas de usuário locais somente em casos especiais quando não for possível usar contas de usuário de domínio.

7. Clique **OK**.

9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como adicionar regras de impressão no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador → Controle de dispositivos**.

2. no painel de resultados do node **Controle de dispositivos**, clique no link **Propriedades**.

   A janela **Propriedades: Controle de dispositivos** é aberta.

3. Marque a caixa de seleção **Controle de dispositivos**.

4. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.

5. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.

6. Configurar as regras de acesso à impressora:

   a. Para os tipos dr dispositivo **Impressoras locais** e **Impressoras de rede**, configure as regras de acesso: **Permitir**, **Bloquear**, **Permitir e não registrar** (somente impressoras de rede), **Depende do barramento de conexão** (somente impressoras locais), **Por regras**.

   b. Caso o modo de acesso **Depende do barramento de conexão** seja selecionado, será necessário configurar regras de acesso para as interfaces de conexão na guia **Barramentos de conexão**.

   c. Caso o modo de acesso **Por regras** seja selecionado, será necessário configurar as regras de impressão:

      1. Clique duas vezes nos tipos de dispositivo **Impressoras locais** e **Impressoras de rede** para abrir as propriedades da regra de acesso.

      2. Selecione os usuários ou grupo de usuários para os quais deseja aplicar a regra de impressão. Para isso, clique no botão **Adicionar**.

         Uma janela será exibida para adicionar uma nova regra de impressão.

      3. Atribua uma prioridade à *entrada da regra*. Uma entrada de regra inclui os seguintes atributos: conta de usuário, ação (permitir/bloquear) e prioridade.

         Uma regra tem uma prioridade específica. Se um usuário foi adicionado a vários grupos, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Embedded Systems Security permite a atribuição de 0 a 10.000. Quanto mais alto for o valor, maior é a prioridade. Em outras palavras, uma entrada com o valor 0 possui a prioridade mais baixa.

Por exemplo, você pode conceder permissões de somente leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para fazer isso, atribua uma prioridade de 1 para o grupo de administradores e atribua uma prioridade de 0 para o grupo Todos.

A prioridade da regra de bloqueio é mais alta do que a de permissão. Em outras palavras, se um usuário foi adicionado a vários grupos e a prioridade de todas as regras é a mesma, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

4. Em **Ação**, configure o acesso do usuário para imprimir na impressora.

5. Clique em **Usuários e grupos** e selecione usuários ou grupos de usuários para acessar a impressão. É possível selecionar usuários no Active Directory, na lista de contas no Kaspersky Security Center ou ao inserir um nome de usuário local manualmente. A Kaspersky recomenda usar contas de usuário locais somente em casos especiais quando não for possível usar contas de usuário de domínio.

6. Clique **OK**.

7. Salvar alterações.

Entrada do controle de dispositivos (HID)

Os dispositivos de entrada consistem em teclados, mouses, trackballs, touchpads e outros dispositivos semelhantes. É possível conectar dispositivos de entrada usando as seguintes interfaces: USB, Bluetooth, porta PS/2, porta RS-232 (COM), porta IR, etc.

O Kaspersky Embedded Systems Security permite controlar mouses e teclados USB e Bluetooth. O Controle de Dispositivos registra em log os dispositivos de conexão e desconexão de dispositivos de entrada.

Quando os dispositivos Bluetooth estão conectados ou desconectados, o aplicativo pode criar vários eventos em relação o dispositivo. O motivo é que o sistema operacional pode detectar um dispositivo Bluetooth como vários dispositivos de tipos diferentes. O Kaspersky Embedded Systems Security também gerencia o adaptador Bluetooth por meio do qual o dispositivo está conectado como um dispositivo separado. É por isso que o aplicativo cria um evento para cada um dos dispositivos detectados.

O Kaspersky Embedded Systems Security deixa que você permita ou proíba o uso de um dispositivo de entrada, além de criar uma lista de dispositivos confiáveis.

Como ativar o Controle de dispositivos no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controle de atividades locais**.

4. Na seção **Controle de dispositivos**, clique no botão **Configurações**.

5. Marque a caixa de seleção **Controle de dispositivos**.

6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.
7. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A guia **Tipos de dispositivos** exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente Controle de Dispositivos.
8. Para o tipo de dispositivo **Bluetooth**, selecione um modo de acesso: **Permitir**, **Bloquear**, **Permitir e não registrar**.

   É possível bloquear ou permitir todos os dispositivos Bluetooth ou permitir a conexão apenas para os dispositivos de entrada Bluetooth (classe HID (Dispositivos de Interface Humana)).

   > É possível permitir a conexão de dispositivos de entrada somente no Kaspersky Security Center Web Console. Não é possível permitir a conexão de dispositivos de entrada no Console de Administração (MMC).
9. Para os tipos de dispositivo **Teclados USB** e **Mouses USB**, selecione um modo de acesso: **Permitir**, **Bloquear**, **Depende do barramento de conexão**.
10. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como ativar o Controle de dispositivos no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controle de atividades locais** → **Controle de dispositivos** e clique no botão **Configurar**.

   A janela **Controle de dispositivos** é aberta.
5. Marque a caixa de seleção **Ativar o Controle de dispositivos**.
6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.
7. No bloco **Configurações do Controle de dispositivos**, clique em **Regras de acesso para dispositivos e redes Wi-Fi**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.
8. Clique no tipo de dispositivo **Bluetooth** para abrir as propriedades da regra de acesso.
9. Selecione um modo de acesso: **Permitir**, **Bloquear**, **Permitir e não registrar**.

   É possível bloquear ou permitir todos os dispositivos Bluetooth ou permitir a conexão apenas para os dispositivos de entrada Bluetooth (classe HID (Dispositivos de Interface Humana)).

10. Para os tipos de dispositivo **Teclados USB** e **Mouses USB**, selecione um modo de acesso: **Permitir**, **Bloquear**, **Depende do barramento de conexão**.
11. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como configurar o Controle de dispositivos no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Controle de dispositivos**.
2. no painel de resultados do node **Controle de dispositivos**, clique no link **Propriedades**.

   A janela **Propriedades: Controle de dispositivos** é aberta.
3. Marque a caixa de seleção **Controle de dispositivos**.
4. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.
5. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.
6. Para o tipo de dispositivo **Bluetooth**, selecione um modo de acesso: **Permitir**, **Bloquear**, **Permitir e não registrar**.

   É possível bloquear ou permitir todos os dispositivos Bluetooth ou permitir a conexão apenas para os dispositivos de entrada Bluetooth (classe HID (Dispositivos de Interface Humana)).

   > É possível permitir a conexão de dispositivos de entrada somente no Kaspersky Security Center Web Console. Não é possível permitir a conexão de dispositivos de entrada no Console de Administração (MMC).
7. Para os tipos de dispositivo **Teclados USB** e **Mouses USB**, selecione um modo de acesso: **Permitir**, **Bloquear**, **Depende do barramento de conexão**.
8. Salvar alterações.

Monitorar o uso de unidades removíveis

O monitoramento do uso de unidades removíveis inclui:

- Monitoramento das operações em arquivos em unidades removíveis.
- Monitoramento da conexão e desconexão de unidades removíveis confiáveis.

  O Kaspersky Embedded Systems Security permite o monitoramento da conexão e a desconexão de todos os dispositivos confiáveis e não apenas das unidades removíveis. É possível ativar o login de eventos configurações de notificação para o componente de Controle de Dispositivos. Os eventos têm o nível de gravidade *Informativo*.

Como ativar o monitoramento de operações de arquivos em unidades removíveis no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controle de atividades locais**.
4. Na seção **Controle de dispositivos**, clique no botão **Configurações**.
5. Marque a caixa de seleção **Controle de dispositivos**.
6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.
7. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A guia **Tipos de dispositivos** exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente Controle de Dispositivos.
8. Selecione o tipo de dispositivo **Unidades removíveis** e clique no botão **Criação de log**.

   Essa ação abre a janela da senha do administrador.
9. Marque a caixa de seleção **Ativar registro em log**.
10. No bloco **Operações com arquivos**, selecione as operações que deseja monitorar: **Gravar**, **Excluir**.
11. Na seção **Filtrar por formatos de arquivo**, selecione os formatos de arquivos cujas operações associadas devem ser registradas pelo Controle de Dispositivos.
12. Selecione os usuários ou grupo de usuários cujo uso de unidades removíveis você deseja monitorar.
13. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como ativar o monitoramento de operações de arquivos em unidades removíveis no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controle de atividades locais** → **Controle de dispositivos** e clique no botão **Configurar**.

   A janela **Controle de dispositivos** é aberta.
5. Marque a caixa de seleção **Ativar o Controle de dispositivos**.
6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.

7. No bloco **Configurações do Controle de dispositivos**, clique em **Regras de acesso para dispositivos e redes Wi-Fi**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.

8. Clique duas vezes no tipo de dispositivo **Unidades removíveis** para abrir as propriedades da regra de acesso.

9. Na janela que é aberta, selecione a guia **Criação de log**.

10. Defina o botão de alternância para **Criação de log ATIVADA**.

11. No bloco **Operações com arquivos**, selecione as operações que deseja monitorar: **Gravar**, **Excluir**.

12. Na seção **Filtrar por formatos de arquivo**, selecione os formatos de arquivos cujas operações associadas devem ser registradas pelo Controle de Dispositivos.

13. Selecione os usuários ou grupo de usuários cujo uso de unidades removíveis você deseja monitorar.

14. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como ativar o monitoramento de operações de arquivos em unidades removíveis no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Controle de dispositivos**.

2. no painel de resultados do node **Controle de dispositivos**, clique no link **Propriedades**.

   A janela **Propriedades: Controle de dispositivos** é aberta.

3. Marque a caixa de seleção **Controle de dispositivos**.

4. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.

5. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.

6. Selecione o tipo de dispositivo **Unidades removíveis** e clique no botão **Criação de log**.

   Essa ação abre a janela da senha do administrador.

7. Marque a caixa de seleção **Ativar registro em log**.

8. No bloco **Operações com arquivos**, selecione as operações que deseja monitorar: **Gravar**, **Excluir**.

9. Na seção **Filtrar por formatos de arquivo**, selecione os formatos de arquivos cujas operações associadas devem ser registradas pelo Controle de Dispositivos.

10. Selecione os usuários ou grupo de usuários cujo uso de unidades removíveis você deseja monitorar.

11. Salvar alterações.

Como resultado, quando os usuários gravam em arquivos localizados em unidades removíveis ou excluem arquivos de unidades removíveis, o Kaspersky Embedded Systems Security salva as informações sobre tais operações no log de eventos e envia os eventos para o Kaspersky Security Center. É possível visualizar eventos associados com arquivos em unidades removíveis no Console do Kaspersky Security Center, na área de trabalho do nó **Servidor de Administração** na guia **Eventos**. Para que os eventos sejam exibidos no log de eventos do Kaspersky Embedded Systems Security local, é necessário marcar a caixa de seleção **Operação com arquivo realizada** nas configurações de notificações para o componente Controle de Dispositivos.

Gerenciando o acesso a dispositivos Bluetooth

O Kaspersky Embedded Systems Security permite gerenciar o acesso a dispositivos Bluetooth. Os dispositivos Bluetooth incluem teclados sem fio, mouses, fones de ouvido, impressoras, etc. Também é possível usar o Bluetooth para comunicação, por exemplo, com um dispositivo móvel.

Quando os dispositivos Bluetooth estão conectados ou desconectados, o aplicativo pode criar vários eventos em relação o dispositivo. O motivo é que o sistema operacional pode detectar um dispositivo Bluetooth como vários dispositivos de tipos diferentes. O Kaspersky Embedded Systems Security também gerencia o adaptador Bluetooth por meio do qual o dispositivo está conectado como um dispositivo separado. É por isso que o aplicativo cria um evento para cada um dos dispositivos detectados.

É possível selecionar um dos seguintes modos de acesso a dispositivos Bluetooth:

- **Permitir e não registrar** . O Kaspersky Embedded Systems Security permite conectar qualquer dispositivo Bluetooth e não salva as informações em relação à conexão no log de eventos. É possível conectar os dispositivos de entrada Bluetooth (teclados, mouses e etc.), enviar dados por Bluetooth e gerenciar outros dispositivos Bluetooth (fones de ouvido, microfones e etc.).
- **Permitir** . O Kaspersky Embedded Systems Security permite conectar qualquer dispositivo Bluetooth. É possível conectar dispositivos de entrada Bluetooth (teclados, mouses, etc.), enviar dados por Bluetooth e gerenciar outros dispositivos Bluetooth (fones de ouvido, microfones, etc.).
- **Bloquear** . O Kaspersky Embedded Systems Security restringe o acesso aos dispositivos Bluetooth. É possível permitir somente a conexão de dispositivos de entrada Bluetooth (a classe dispositivos de interface humana). Esses dispositivos incluem teclados, mouses, joysticks e etc.

Não é possível criar uma lista de dispositivos Bluetooth confiáveis. Se você restringir o acesso a dispositivos Bluetooth, só poderá conectar dispositivos de entrada Bluetooth.

É possível permitir a conexão de dispositivos de entrada somente no Console do Aplicativo ou no Kaspersky Security Center Web Console. É possível permitir a conexão de dispositivos de entrada somente no Console de Administração do Kaspersky Security Center.

Como configurar as regras de acesso ao dispositivo Bluetooth no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controle de atividades locais** → **Controle de dispositivos** e clique em **Configurações**.

4. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A tabela lista as regras de acesso para todos os dispositivos presentes na classificação do componente Controle de Dispositivos.

5. No menu de contexto do tipo de dispositivo **Bluetooth**, configure o modo de acesso do dispositivo Bluetooth: **Permitir**, **Bloquear** e **Permitir e não registrar**.

   Caso tenha bloqueado o acesso aos dispositivos Bluetooth, é possível permitir somente a conexão de dispositivos de entrada (teclados, mouses, etc.) somente no Console do Aplicativo ou no Kaspersky Security Center Web Console. É possível permitir a conexão de dispositivos de entrada somente no Console de Administração do Kaspersky Security Center.

6. Salvar alterações.

Como configurar as regras de acesso do dispositivo Bluetooth no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Na janela da política, selecione **Controle de atividades locais** → **Controle de dispositivos** e clique em **Configurações**.

5. No bloco **Configurações do Controle de dispositivos**, clique no link **Regras de acesso para dispositivos e redes Wi-Fi**.

   A tabela lista as regras de acesso para todos os dispositivos presentes na classificação do componente Controle de Dispositivos.

6. Selecione o tipo de dispositivo como **Bluetooth**.

   As configurações de acesso ao dispositivo Bluetooth são abertas.

7. Configure o modo de acesso do dispositivo Bluetooth: **Permitir**, **Bloquear** e **Permitir e não registrar**.

8. Caso tenha selecionado o modo **Bloquear**, é possível permitir a conexão apenas de dispositivos de entrada Bluetooth (teclados, mouses, etc.). Para fazer isso, sob **Exclusões**, selecione a caixa de seleção **Dispositivos de entrada (mouses e teclados)**.

9. Salvar alterações.

Como configurar as regras de acesso do dispositivo Bluetooth no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Controle de dispositivos**.
2. no painel de resultados do node **Controle de dispositivos**, clique no link **Propriedades**.

   A janela **Propriedades: Controle de dispositivos** é aberta.
3. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A tabela lista as regras de acesso para todos os dispositivos presentes na classificação do componente Controle de Dispositivos.
4. Em **Acesso**, configure o modo de acesso dos dispositivos Bluetooth: **Permitir**, **Bloquear** e **Permitir e não registrar**.
5. Caso tenha selecionado o modo **Bloquear**, é possível permitir a conexão apenas de dispositivos de entrada Bluetooth (teclados, mouses, etc.). Para fazer isso, sob **Exclusões**, selecione a caixa de seleção **Dispositivos de entrada (mouses e teclados)**.
6. Salvar alterações.

Diferenciação dos direitos de acesso do usuário aos dispositivos

É possível configurar os direitos de acesso do usuário por tipo de dispositivo ou acesso aos dispositivos confiáveis.

Diferenciação dos direitos de acesso do usuário por tipo de dispositivo

O controle de dispositivos permite configurar os direitos de acesso do usuário aos dados em *dispositivos de armazenamento*. Para esses dispositivos, é possível configurar as permissões de leitura e gravação. O controle de dispositivos é compatível com os seguintes tipos de dispositivos de armazenamento:

- Discos rígidos
- Unidade removível
- Disquetes
- Unidades de CD/DVD-ROM
- Dispositivos portáteis (MTP) incluem, por exemplo, dispositivos móveis, câmeras fotográficas, reprodutores de mídia, etc.

Isso significa que é possível, por exemplo, permitir o uso de unidades removíveis apenas para o grupo de administradores. Para outros tipos de dispositivos, é possível negar ou permitir o acesso de todos os usuários. Também é possível configurar os direitos de acesso do usuário a impressoras.

Como configurar os direitos de acesso do usuário aos dados em unidades removíveis no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controle de atividades locais**.
4. Na seção **Controle de dispositivos**, clique no botão **Configurações**.
5. Marque a caixa de seleção **Controle de dispositivos**.
6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.
7. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A guia **Tipos de dispositivos** exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente Controle de Dispositivos.
8. Para configurar regras de acesso a dispositivos móveis, clique duas vezes para abrir a lista de regras.
9. Configure a regra de acesso do dispositivo móvel:

   a. No bloco **Regras de acesso**, clique no botão **Adicionar**.

      Uma janela se abrirá para adicionar uma nova regra de acesso ao dispositivo móvel.

   b. No campo **Prioridade**, defina a prioridade da *entrada da regra*. Uma regra inclui os seguintes atributos: conta do usuário, programação, permissões (leitura/gravação) e prioridade.

      Uma regra tem uma prioridade específica. Se um usuário foi adicionado a vários grupos, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Embedded Systems Security permite a atribuição de 0 a 10.000. Quanto mais alto for o valor, maior é a prioridade. Em outras palavras, uma entrada com o valor 0 possui a prioridade mais baixa.

      Por exemplo, você pode conceder permissões de somente leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para fazer isso, atribua uma prioridade de 1 para o grupo de administradores e atribua uma prioridade de 0 para o grupo Todos.

      A prioridade da regra de bloqueio é mais alta do que a de permissão. Em outras palavras, se um usuário foi adicionado a vários grupos e a prioridade de todas as regras é a mesma, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

   c. Em **Regra para usuários e grupos**, selecione usuários ou grupos de usuários. É possível selecionar usuários no Active Directory, na lista de contas no Kaspersky Security Center ou ao inserir um nome de usuário local manualmente. A Kaspersky recomenda usar contas de usuário locais somente em casos especiais quando não for possível usar contas de usuário de domínio.

   d. Clique **OK**.
10. Em **Agendamentos para a regra de acesso selecionada**, configure um agendamento de acesso ao dispositivo de armazenamento para os usuários.

    Por exemplo, é possível permitir o acesso do usuário aos dispositivos de armazenamento durante o horário de trabalho apenas.

11. Configure as permissões de acesso dos usuários a dispositivos de armazenamento no gerenciador de arquivos (**Ler**/**Gravar**).

12. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como configurar os direitos de acesso do usuário aos dados em dispositivos de armazenamento no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Vá para **Controle de atividades locais** → **Controle de dispositivos** e clique no botão **Configurar**.

   A janela **Controle de dispositivos** é aberta.

5. Marque a caixa de seleção **Ativar o Controle de dispositivos**.

6. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.

7. No bloco **Configurações do Controle de dispositivos**, clique em **Regras de acesso para dispositivos e redes Wi-Fi**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.

8. No bloco **Acesso a dispositivos de armazenamento**, abra as propriedades da regra de acesso ao dispositivo de armazenamento.

9. Configure a regra de acesso do dispositivo móvel:

   a. No bloco **Usuários**, clique no botão **Adicionar**.

      Uma janela se abrirá para adicionar uma nova regra de acesso ao dispositivo móvel.

   b. No campo **Prioridade**, defina a prioridade da *entrada da regra*. Uma regra inclui os seguintes atributos: conta do usuário, programação, permissões (leitura/gravação) e prioridade.

      Uma regra tem uma prioridade específica. Se um usuário foi adicionado a vários grupos, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Embedded Systems Security permite a atribuição de 0 a 10.000. Quanto mais alto for o valor, maior é a prioridade. Em outras palavras, uma entrada com o valor 0 possui a prioridade mais baixa.

      Por exemplo, você pode conceder permissões de somente leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para fazer isso, atribua uma prioridade de 1 para o grupo de administradores e atribua uma prioridade de 0 para o grupo Todos.

      A prioridade da regra de bloqueio é mais alta do que a de permissão. Em outras palavras, se um usuário foi adicionado a vários grupos e a prioridade de todas as regras é a mesma, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

c. Em **Usuários**, selecione usuários ou grupos de usuários. É possível selecionar usuários no Active Directory, na lista de contas no Kaspersky Security Center ou ao inserir um nome de usuário local manualmente. A Kaspersky recomenda usar contas de usuário locais somente em casos especiais quando não for possível usar contas de usuário de domínio.

d. Em **Agendamento para acesso a dispositivos**, configure um agendamento de acesso ao dispositivo de armazenamento para os usuários.

Por exemplo, é possível permitir o acesso do usuário aos dispositivos de armazenamento durante o horário de trabalho apenas.

e. Configure as permissões de acesso dos usuários a dispositivos de armazenamento no gerenciador de arquivos (**Ler**/**Gravar**).

f. Clique **OK**.

10. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como configurar os direitos de acesso do usuário aos dados em dispositivos de armazenamento no Kaspersky Embedded Systems Security Console

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Controle de dispositivos**.
2. no painel de resultados do node **Controle de dispositivos**, clique no link **Propriedades**.

   A janela **Propriedades: Controle de dispositivos** é aberta.
3. Marque a caixa de seleção **Controle de dispositivos**.
4. No bloco **Modo de operação para regras de bloqueio**, selecione **Bloquear** ou **Informar**.
5. Em **Configurações do controle de dispositivos**, selecione a guia **Tipos de dispositivos**.

   A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.
6. Para configurar regras de acesso a dispositivos móveis, clique duas vezes para abrir a lista de regras.
7. Configure a regra de acesso do dispositivo móvel:

   a. No bloco **Regras de acesso**, clique no botão **Adicionar**.

   Uma janela se abrirá para adicionar uma nova regra de acesso ao dispositivo móvel.

   b. No campo **Prioridade da regra**, defina a prioridade da *entrada da regra*. Uma regra inclui os seguintes atributos: conta do usuário, programação, permissões (leitura/gravação) e prioridade.

   Uma regra tem uma prioridade específica. Se um usuário foi adicionado a vários grupos, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Embedded Systems Security permite a atribuição de 0 a 10.000. Quanto mais alto for o valor, maior é a prioridade. Em outras palavras, uma entrada com o valor 0 possui a prioridade mais baixa.

   Por exemplo, você pode conceder permissões de somente leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para fazer isso, atribua uma prioridade de 1 para o grupo de administradores e atribua uma prioridade de 0 para o grupo Todos.

A prioridade da regra de bloqueio é mais alta do que a de permissão. Em outras palavras, se um usuário foi adicionado a vários grupos e a prioridade de todas as regras é a mesma, o Kaspersky Embedded Systems Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

c. Em **Regra para usuários e grupos**, selecione usuários ou grupos de usuários. É possível selecionar os usuários no Active Directory ou inserir manualmente um nome de usuário local. A Kaspersky recomenda usar contas de usuário locais somente em casos especiais quando não for possível usar contas de usuário de domínio.

d. Clique **OK**.

8. Em **Agendamentos para a regra de acesso selecionada**, configure um agendamento de acesso ao dispositivo de armazenamento para os usuários.

   Por exemplo, é possível permitir o acesso do usuário aos dispositivos de armazenamento durante o horário de trabalho apenas.

9. Configure as permissões de acesso dos usuários a dispositivos de armazenamento no gerenciador de arquivos (**Ler**/**Gravar**).

10. Salvar alterações.

Diferenciação dos direitos de acesso do usuário aos dispositivos confiáveis

Dispositivos confiáveis aqueles aos quais os usuários especificados têm acesso total a qualquer momento. Para trabalhar com dispositivos confiáveis, você pode conceder acesso a um usuário individual, a um grupo de usuários ou a todos os usuários da organização. É possível configurar os direitos de acesso nas propriedades do dispositivo confiável.

Auditoria de dispositivo externa

Para criar uma lista de dispositivos confiáveis, é necessário realizar uma auditoria dos dispositivos externos em sua organização. Para adicionar um dispositivo confiável, é necessário selecionar um dispositivo conectado e atribuir o status de confiável ao dispositivo. É possível obter uma lista de dispositivos das seguintes maneiras:

- Ativar o Controle de dispositivos no modo Informar.

  Como ativar o Controle de dispositivo no modo Informar no Console de Administração do Kaspersky Security Center

  1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
  2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
  3. Na janela da política, selecione **Controle de atividades locais**.
  4. Na seção **Controle de dispositivos**, clique no botão **Configurações**.
  5. Marque a caixa de seleção **Controle de dispositivos**.

6. Em **Modo de operação para regras de bloqueio**, selecione **Informar**.
7. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como ativar o Controle de dispositivos no modo Informar no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controle de atividades locais** → **Controle de dispositivos** e clique no botão **Configurar**.
   A janela **Controle de dispositivos** é aberta.
5. Marque a caixa de seleção **Ativar o Controle de dispositivos**.
6. Em **Modo de operação para regras de bloqueio**, selecione **Informar**.
7. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como ativar o Controle de dispositivos no modo Informar no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Controle de dispositivos**.
2. no painel de resultados do node **Controle de dispositivos**, clique no link **Propriedades**.
   A janela **Propriedades: Controle de dispositivos** é aberta.
3. Marque a caixa de seleção **Controle de dispositivos**.
4. Em **Modo de operação para regras de bloqueio**, selecione **Informar**.
5. Salvar alterações.

Assim, o Kaspersky Embedded Systems Security registrará os eventos de conexão e desconexão de dispositivos externos. Em seguida, é possível gerar um relatório de equipamentos e, após analisar o relatório, adicionar dispositivos confiáveis.

- Execute a tarefa *Gerador de Regras de Controle de Dispositivos*.

  Como executar a tarefa Gerador de Regras de Controle de Dispositivos no Console de Administração do Kaspersky Security Center

  1. Abra o Console de Administração do Kaspersky Security Center.
  2. Na árvore do console, selecione **Tarefas**.

3. Selecione a tarefa *Gerador de Regras de Controle de Dispositivos* e clique duas vezes para abrir as propriedades dela.

   Caso seja necessário, crie um novo pacote de instalação.

4. Na seção **Modo**, selecione o modo da tarefa:

   - **Considerar dados do sistema de todos os dispositivos externos que já foram conectados**.

     O aplicativo obtém informações sobre todos os dispositivos que foram conectados ao computador por meio da memória do sistema operacional.

   - **Considerar somente dispositivos externos conectados no momento**.

     O aplicativo obtém informações sobre os dispositivos conectados quando a tarefa é iniciada.

5. Insira o caminho onde deseja salvar o arquivo com os dados.

6. Caso execute a tarefa em vários computadores, recomendamos marcar a caixa de seleção **Adicionar os detalhes sobre o dispositivo protegido ao nome do arquivo**.

7. Salvar alterações.

8. Execute a tarefa.

Como executar a tarefa Gerador de Regras de Controle de Dispositivos no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Tarefas**.

   A lista de tarefas é aberta.

2. Selecione a tarefa *Gerador de Regras de Controle de Dispositivos* e clique duas vezes para abrir as propriedades dela.

   Caso seja necessário, crie um novo pacote de instalação.

3. Na seção **Modo**, selecione o modo da tarefa:

   - **Considerar dados do sistema de todos os dispositivos externos que já foram conectados**.

     O aplicativo obtém informações sobre todos os dispositivos que foram conectados ao computador por meio da memória do sistema operacional.

   - **Considerar somente dispositivos externos conectados no momento**.

     O aplicativo obtém informações sobre os dispositivos conectados quando a tarefa é iniciada.

4. Insira o caminho onde deseja salvar o arquivo com os dados.

5. Caso execute a tarefa em vários computadores, recomendamos marcar a caixa de seleção **Adicionar os detalhes sobre o dispositivo protegido ao nome do arquivo**.

6. Salvar alterações.

7. Execute a tarefa.

[Como iniciar a tarefa Gerador de Regras de Controle de Dispositivos no Console do Aplicativo]

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Geração de regra automática → Gerador de Regras de Controle de Dispositivos**.
2. no painel de resultados do node **Gerador de Regras de Controle de Dispositivos**, clique no link **Propriedades**.

   A janela **Propriedades: Gerador de Regras de Controle de Dispositivos** é aberta.
3. Na seção **Modo**, selecione o modo da tarefa:

   - **Considerar dados do sistema de todos os dispositivos externos que já foram conectados**.

     O aplicativo obtém informações sobre todos os dispositivos que foram conectados ao computador por meio da memória do sistema operacional.

   - **Considerar somente dispositivos externos conectados no momento**.

     O aplicativo obtém informações sobre os dispositivos conectados quando a tarefa é iniciada.
4. Na seção **Após a conclusão da tarefa**, selecione as ações do aplicativo após a conclusão da tarefa:

   - **Adicionar regras de permissão à lista de regras de Controle de Dispositivos**. A lista de regras de Controle de Dispositivos está disponível nas configurações de Controle de Dispositivos.

     Se a caixa de seleção estiver marcada, o aplicativo adicionará as regras geradas pela tarefa à lista de regras de Controle de Dispositivos com base no princípio selecionado para adição de regras.

     Se essa caixa de seleção estiver desmarcada, o aplicativo não adicionará as regras de permissão geradas recentemente à lista de regras de Controle de Dispositivos. O aplicativo só exporta regras para um arquivo.

   - **Princípio da adição**. Um método usado para adicionar as regras de permissão recém-geradas à lista de regras de Controle de Dispositivos:

     - **Adicionar às regras existentes**. O aplicativo adiciona uma regra à lista de regras existentes. Nesse caso, o aplicativo duplica regras idênticas.
     - **Substituir as regras existentes**. O aplicativo adiciona novas regras em vez de regras existentes.
     - **Mesclar com as regras existentes**. O aplicativo adiciona uma regra à lista de regras existentes. Nesse caso, o aplicativo mescla regras idênticas.

   - **Exportar regras de permissão para o arquivo**. O aplicativo exporta regras de permissão para o arquivo especificado no campo abaixo. É possível, então, importar o arquivo nas configurações do aplicativo em outros computadores para distribuir as regras de permissão. O arquivo também pode ser usado para fazer backup das regras de permissão.

   - **Adicionar os detalhes sobre o dispositivo protegido ao nome do arquivo**. Além de data e hora, o aplicativo adiciona o nome do computador ao nome do arquivo exportado. É conveniente coletar regras de permissão de vários computadores.
5. Salvar alterações.

Assim, o Kaspersky Embedded Systems Security realiza uma auditoria de dispositivos externos e salva as informações no registro do Kaspersky Security Center. A lista de dispositivos externos está disponível durante a adição de dispositivos confiáveis.

Adicionar processos confiáveis

Dispositivos confiáveis aqueles aos quais os usuários especificados têm acesso total a qualquer momento.

Para trabalhar com dispositivos confiáveis, você pode conceder acesso a um usuário individual, a um grupo de usuários ou a todos os usuários da organização.

Por exemplo, se sua organização não permitir o uso de unidades removíveis, mas os administradores usarem unidades removíveis em seu trabalho, você poderá permitir unidades removíveis apenas para um grupo de administradores. Para fazer isso, adicione unidades removíveis à lista confiável e configure as permissões de acesso do usuário.

Não é recomendado adicionar mais de 1.000 dispositivos confiáveis, pois isso pode causar instabilidade no sistema.

Como adicionar um dispositivo confiável no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controle de atividades locais**.
4. Na seção **Controle de dispositivos**, clique no botão **Configurações**.
5. Em **Configurações de monitoramento de dispositivos**, selecione a guia **Dispositivos confiáveis**.

   A lista de dispositivos confiáveis é aberta.
6. Marque a caixa de seleção **Mesclar valores ao herdar** se desejar criar uma lista consolidada de dispositivos confiáveis para todos os computadores da empresa.

   As listas de dispositivos confiáveis nas políticas pai e filho serão mescladas. As listas serão mescladas, desde que a mesclagem de valores ao herdar esteja ativada. Dispositivos confiáveis da política pai são exibidos nas políticas filho em uma exibição somente leitura. Não é possível alterar ou excluir dispositivos confiáveis da política pai.
7. Clique no botão **Adicionar** e selecione um método para adicionar um dispositivo à lista confiável:

   - **Gerar regras com base nos dispositivos conectados**.
   - **Gerar regras com base nos dados do sistema**.
   - **Gerar as regras de acordo com o registro do Kaspersky Security Center**.

   Caso a lista de dispositivos esteja vazia, será necessário realizar uma auditoria de dispositivos externos. Para isso, execute a tarefa *Gerador de Regras de Controle de Dispositivos*.

O Kaspersky Embedded Systems Security não é compatível com a adição de dispositivos do tipo **Disquetes** na lista de dispositivos confiáveis.

8. Clique **Adicionar regras para dispositivos selecionados**.
9. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como adicionar um dispositivo confiável no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controle de atividades locais** → **Controle de dispositivos** e clique no botão **Configurar**.

   A janela **Controle de dispositivos** é aberta.
5. No bloco **Configurações do Controle de dispositivos**, clique em **Dispositivos confiáveis**.

   A lista de dispositivos confiáveis é aberta.
6. Marque a caixa de seleção **Mesclar valores ao herdar** se desejar criar uma lista consolidada de dispositivos confiáveis para todos os computadores da empresa.

   As listas de dispositivos confiáveis nas políticas pai e filho serão mescladas. As listas serão mescladas, desde que a mesclagem de valores ao herdar esteja ativada. Dispositivos confiáveis da política pai são exibidos nas políticas filho em uma exibição somente leitura. Não é possível alterar ou excluir dispositivos confiáveis da política pai.
7. Clique **Do registro KSC**.

   Caso a lista de dispositivos esteja vazia, será necessário realizar uma auditoria de dispositivos externos. Para isso, execute a tarefa *Gerador de Regras de Controle de Dispositivos*.

   O Kaspersky Embedded Systems Security não é compatível com a adição de dispositivos do tipo **Disquetes** na lista de dispositivos confiáveis.
8. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como adicionar um dispositivo confiável no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Controle de dispositivos**.
2. no painel de resultados do node **Controle de dispositivos**, clique no link **Propriedades**.

   A janela **Propriedades: Controle de dispositivos** é aberta.

3. Em **Configurações do controle de dispositivos**, selecione a guia **Dispositivos confiáveis**.

   A lista de dispositivos confiáveis é aberta.

4. Clique no botão **Adicionar** e selecione um método para adicionar um dispositivo à lista confiável:

   - **Gerar regras com base nos dispositivos conectados**.
   - **Gerar regras com base nos dados do sistema**.
   - **Gerar as regras de acordo com o registro do Kaspersky Security Center**.

   Caso a lista de dispositivos esteja vazia, será necessário realizar uma auditoria de dispositivos externos. Para isso, execute a tarefa *Gerador de Regras de Controle de Dispositivos*.

   > O Kaspersky Embedded Systems Security não é compatível com a adição de dispositivos do tipo **Disquetes** na lista de dispositivos confiáveis.

5. Clique **Adicionar regras para dispositivos selecionados**.

6. Salvar alterações.

Exportação e importação da lista de dispositivos confiáveis

Para distribuir a lista de dispositivos confiáveis para outros computadores da organização, você pode usar o procedimento de exportação/importação. É possível exportar a lista de dispositivos confiáveis para um arquivo XML. Em seguida, será possível modificar o arquivo para, por exemplo, adicionar um grande número de dispositivos do mesmo tipo. Você pode usar a função de exportação/importação para fazer backup da lista de dispositivos confiáveis ou para migrar a lista para um servidor diferente.

> O Kaspersky Embedded Systems Security permite importar a lista de dispositivos confiáveis do Kaspersky Endpoint Security for Windows. O formato de arquivo XML para esses aplicativos é o mesmo.

Como exportar e importar uma lista de dispositivos confiáveis no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controle de atividades locais**.
4. Na seção **Controle de dispositivos**, clique no botão **Configurações**.
5. Em **Configurações do controle de dispositivos**, selecione a guia **Dispositivos confiáveis**.

   A lista de dispositivos confiáveis é aberta.

6. Para exportar a lista de dispositivos confiáveis:

   a. Selecione os dispositivos confiáveis que deseja exportar.

   b. Clique no botão e selecione o modo de exportação: exportar a lista completa de dispositivos confiáveis ou apenas os dispositivos confiáveis selecionados.

   c. Na janela exibida, selecione um arquivo de configuração, especifique o nome do arquivo XML para o qual você quer exportar a lista de dispositivos confiáveis, selecione a pasta na qual você quer salvar esse arquivo.

   d. Salvar o arquivo.

      O Kaspersky Embedded Systems Security exporta a lista de endereços de recursos da web para um arquivo XML.

7. Para importar a lista de dispositivos confiáveis:

   a. Clique em **Adicionar** → **Importar regras do arquivo XML** e selecione um modo de importação: adicionar ou substituir.

      Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de recursos da Web.

      No modo mesclar, o aplicativo verificará as listas de dispositivos confiáveis e removerá as entradas duplicadas. No modo adicionar, o aplicativo adicionará entradas na lista de aplicativos confiáveis sem verificar se há duplicatas.

   b. Abra o arquivo.

      O Kaspersky Embedded Systems Security importa dispositivos confiáveis de acordo com o modo selecionado.

8. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como exportar e importar uma lista de dispositivos confiáveis no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controle de atividades locais** → **Controle de dispositivos** e clique no botão **Configurar**.

   A janela **Controle de dispositivos** é aberta.
5. No bloco **Configurações do Controle de dispositivos**, clique em **Dispositivos confiáveis**.

   A lista de dispositivos confiáveis é aberta.
6. Para exportar a lista de dispositivos confiáveis:

   a. Selecione os dispositivos confiáveis que deseja exportar.

   b. Clique no botão **Exportar** e selecione o modo de exportação: exportar a lista completa de dispositivos confiáveis ou apenas os dispositivos confiáveis selecionados.

c. Salvar o arquivo.

O Kaspersky Embedded Systems Security exporta a lista de endereços de recursos da web para um arquivo XML.

7. Para importar a lista de dispositivos confiáveis:

a. Clique no botão **Importar** e selecione um modo de importação: adicionar ou substituir.

b. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de recursos da Web.

c. Abra o arquivo.

O Kaspersky Embedded Systems Security importa dispositivos confiáveis de acordo com o modo selecionado.

8. Salvar alterações. Para aplicar a política em computadores, feche os cadeados.

Como exportar e importar uma lista de dispositivos confiáveis no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Controle de dispositivos**.

2. no painel de resultados do node **Controle de dispositivos**, clique no link **Propriedades**.

A janela **Propriedades: Controle de dispositivos** é aberta.

3. Em **Configurações do controle de dispositivos**, selecione a guia **Dispositivos confiáveis**.

A lista de dispositivos confiáveis é aberta.

4. Para exportar a lista de dispositivos confiáveis:

a. Selecione os dispositivos confiáveis que deseja exportar.

b. Clique no botão e selecione o modo de exportação: exportar a lista completa de dispositivos confiáveis ou apenas os dispositivos confiáveis selecionados.

c. Na janela exibida, selecione um arquivo de configuração, especifique o nome do arquivo XML para o qual você quer exportar a lista de dispositivos confiáveis, selecione a pasta na qual você quer salvar esse arquivo.

d. Salvar o arquivo.

O Kaspersky Embedded Systems Security exporta a lista de endereços de recursos da web para um arquivo XML.

5. Para importar a lista de dispositivos confiáveis:

a. Clique em **Adicionar** → **Importar regras do arquivo XML** e selecione um modo de importação: adicionar ou substituir.

Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de recursos da Web.

No modo mesclar, o aplicativo verificará as listas de dispositivos confiáveis e removerá as entradas duplicadas. No modo adicionar, o aplicativo adicionará entradas na lista de aplicativos confiáveis sem verificar se há duplicatas.

b. Abra o arquivo.

O Kaspersky Embedded Systems Security importa dispositivos confiáveis de acordo com o modo selecionado.

6. Salvar alterações.

Firewall

O componente de Firewall pode ser executado nos seguintes modos:

- **Observar o estado do Firewall do Windows**. Esse modo tem como objetivo garantir uma transição suave da lógica da tarefa de gerenciamento de Firewall das versões 3.4 e anteriores para o Firewall completo disponível a partir da versão 4.0. As regras da tarefa de gerenciamento de Firewall integradas ao Firewall do Windows são mantidas ao atualizar a versão 3.4, ou suas anteriores. Mas, o componente Firewall não interage mais com o Firewall do Windows, passando a monitorar a filtragem de tráfego e registrar os eventos relacionados no log de operação do componente. No entanto, você pode criar regras de Firewall e/ou importá-las do Firewall do Windows e alterar o modo operacional do Firewall para **Informar**.

- **Informar**. O aplicativo só monitora a operação das regras de Firewall e registra os eventos relacionados no log de operação do componente. É um modo que visa testar as regras do Firewall. Você pode avaliar sua aplicabilidade através do log de operação do Firewall. E, se necessário, ajustar as regras do Firewall e alterar seu modo de operação para **Bloquear**.

- **Bloquear**. O aplicativo filtra o tráfego de rede considerando as configurações do componente e registra os eventos relacionados no log de operação do componente.

Sobre as Regras de Firewall

Se o modo **Bloquear** estiver ativado, o componente do Firewall filtra o tráfego de rede a partir das regras de 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 para acionar essas regras podem incluir o tipo de protocolo, uma porta específica ou um intervalo de portas.

> 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 computador protegido é reduzido.

Configurando o Firewall

Esta seção fornece instruções sobre como definir as configurações gerais do componente de Firewall, além de criar e configurar as regras de Firewall.

Definir configurações gerais de tarefas

Definindo as configurações gerais do componente de Firewall no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na seção **Controle de atividades de rede**, clique no botão **Configurações** na subseção **Firewall**.

   A janela **Firewall** é aberta.
4. Na guia **Geral** no bloco **Modo de operação para regras de bloqueio**, selecione o modo de operação do componente:

   - **Observar o estado do Firewall do Windows**. Esse modo tem como objetivo garantir uma transição suave da lógica da tarefa de gerenciamento de Firewall das versões 3.4 e anteriores para o Firewall completo disponível a partir da versão 4.0. As regras da tarefa de gerenciamento de Firewall integradas ao Firewall do Windows são mantidas ao atualizar a versão 3.4, ou suas anteriores. Mas, o componente Firewall não interage mais com o Firewall do Windows, passando a monitorar a filtragem de tráfego e registrar os eventos relacionados no log de operação do componente. No entanto, você pode criar regras de Firewall e/ou importá-las do Firewall do Windows e alterar o modo operacional do Firewall para **Informar**.

   - **Informar**. O aplicativo só monitora a operação das regras de Firewall e registra os eventos relacionados no log de operação do componente. É um modo que visa testar as regras do Firewall. Você pode avaliar sua aplicabilidade através do log de operação do Firewall. E, se necessário, ajustar as regras do Firewall e alterar seu modo de operação para **Bloquear**.

   - **Bloquear**. O aplicativo filtra o tráfego de rede considerando as configurações do componente e registra os eventos relacionados no log de operação do componente.
5. No bloco **Conexões de entrada**, configurar as conexões de rede de entrada:

   - Use a lista suspensa **Ação para conexões de entrada** para especificar a ação que o aplicativo deverá executar para todas as conexões de rede de entrada, a menos que isso seja definido de outra forma nas regras de 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 aplicativo permitirá as conexões de rede de entrada que correspondam aos critérios da regra.

6. 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 aplicativo deverá executar para todas as conexões de rede de saída, a menos que isso esteja definido de outra forma nas regras de 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 aplicativo bloqueará as conexões de rede de saída que correspondam aos critérios da regra.

7. Salvar alterações.

O Kaspersky Embedded Systems Security aplica as novas configurações. A data e hora nas quais as configurações foram alteradas são salvas no log de auditoria do sistema.

Definindo as configurações gerais do componente do Firewall no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Na seção **Controle de atividades de rede**, clique no botão **Configurar** na subseção **Firewall**.

   A janela **Firewall** é aberta.

5. Defina o botão de alternância para **Firewall ATIVADO**.

6. No bloco **Modo de operação para regras de bloqueio**, selecione o modo de operação do componente:

   - **Observar o estado do Firewall do Windows**. Esse modo tem como objetivo garantir uma transição suave da lógica da tarefa de gerenciamento de Firewall das versões 3.4 e anteriores para o Firewall completo disponível a partir da versão 4.0. As regras da tarefa de gerenciamento de Firewall integradas ao Firewall do Windows são mantidas ao atualizar a versão 3.4, ou suas anteriores. Mas, o componente Firewall não interage mais com o Firewall do Windows, passando a monitorar a filtragem de tráfego e registrar os eventos relacionados no log de operação do componente. No entanto, você pode criar regras de Firewall e/ou importá-las do Firewall do Windows e alterar o modo operacional do Firewall para **Informar**.

   - **Informar**. O aplicativo só monitora a operação das regras de Firewall e registra os eventos relacionados no log de operação do componente. É um modo que visa testar as regras do Firewall. Você pode avaliar sua aplicabilidade através do log de operação do Firewall. E, se necessário, ajustar as regras do Firewall e alterar seu modo de operação para **Bloquear**.

   - **Bloquear**. O aplicativo filtra o tráfego de rede considerando as configurações do componente e registra os eventos relacionados no log de operação do componente.

7. No bloco **Conexões de entrada**, configurar as conexões de rede de entrada:

   - Use a lista suspensa **Ação para conexões de entrada** para especificar a ação que o aplicativo deverá executar para todas as conexões de rede de entrada, a menos que isso seja definido de outra forma nas regras de 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 aplicativo 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 aplicativo deverá executar para todas as conexões de rede de saída, a menos que isso esteja definido de outra forma nas regras de 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 aplicativo bloqueará as conexões de rede de saída que correspondam aos critérios da regra.

9. Salvar alterações.

O Kaspersky Embedded Systems Security aplica as novas configurações. A data e hora nas quais as configurações foram alteradas são salvas no log de auditoria do sistema.

Definindo as configurações gerais do componente de Firewall no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Firewall**.
2. no painel de resultados do node **Firewall**, clique no link **Propriedades**.

   A janela **Propriedades: Firewall** é aberta.
3. Marque a caixa de seleção **Firewall**.

4. No bloco **Modo de operação para regras de bloqueio**, selecione o modo de operação do componente:

   - **Observar o estado do Firewall do Windows**. Esse modo tem como objetivo garantir uma transição suave da lógica da tarefa de gerenciamento de Firewall das versões 3.4 e anteriores para o Firewall completo disponível a partir da versão 4.0. As regras da tarefa de gerenciamento de Firewall integradas ao Firewall do Windows são mantidas ao atualizar a versão 3.4, ou suas anteriores. Mas, o componente Firewall não interage mais com o Firewall do Windows, passando a monitorar a filtragem de tráfego e registrar os eventos relacionados no log de operação do componente. No entanto, você pode criar regras de Firewall e/ou importá-las do Firewall do Windows e alterar o modo operacional do Firewall para **Informar**.

   - **Informar**. O aplicativo só monitora a operação das regras de Firewall e registra os eventos relacionados no log de operação do componente. É um modo que visa testar as regras do Firewall. Você pode avaliar sua aplicabilidade através do log de operação do Firewall. E, se necessário, ajustar as regras do Firewall e alterar seu modo de operação para **Bloquear**.

   - **Bloquear**. O aplicativo filtra o tráfego de rede considerando as configurações do componente e registra os eventos relacionados no log de operação do componente.

5. No bloco **Conexões de entrada**, configurar as conexões de rede de entrada:

   - Use a lista suspensa **Ação para conexões de entrada** para especificar a ação que o aplicativo deverá executar para todas as conexões de rede de entrada, a menos que isso seja definido de outra forma nas regras de 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 aplicativo permitirá as conexões de rede de entrada que correspondam aos critérios da regra.

6. 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 aplicativo deverá executar para todas as conexões de rede de saída, a menos que isso esteja definido de outra forma nas regras de 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 aplicativo bloqueará as conexões de rede de saída que correspondam aos critérios da regra.

7. Salvar alterações.

O Kaspersky Embedded Systems Security aplica as novas configurações. 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

Criando e configurando regras de Firewall no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na seção **Controle de atividades de rede**, clique no botão **Configurações** na subseção **Firewall**.
   A janela **Firewall** é aberta.
4. No bloco **Conexões de entrada**, clique no botão **Lista de regras**.
   A janela **Regras para conexões de entrada** é aberta.
5. Crie e configure as regras do Firewall para as conexões de entrada.

   1. Na guia **Aplicativos**, clique no botão **Adicionar**.
      A janela **Regra para um aplicativo** é aberta.
   2. Defina as configurações da regra:

      a. No campo **Nome da regra**, insira ou edite 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**, 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. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

      d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

      e. 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.

f. No campo **Escopo de uso 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.

> Somente o formato IPv4 é compatível com endereços IP.

g. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

h. Clique no botão **OK** para salvar a regra.

3. Na guia **Portas locais**, clique no botão **Adicionar**.

   A janela **Regra para portas** é aberta.

4. Defina as configurações da regra:

   a. No campo **Nome da regra**, insira ou edite o nome da regra.

   b. Na lista **Ação**, 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. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

   d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

   e. No campo **Escopo de uso 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.

> Somente o formato IPv4 é compatível com endereços IP.

   f. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

   g. Clique no botão **OK** para salvar a regra.

5. Clique no botão **OK** na subseção **Regras para conexões de entrada**.

6. No bloco **Conexões de saída**, clique no botão **Lista de regras**.

   A janela **Regras para conexões de saída** é aberta.

7. Crie e configure as regras do Firewall para as conexões de saída.

   1. Na guia **Aplicativos**, clique no botão **Adicionar**.

      A janela **Regra para um aplicativo** é aberta.

2. Defina as configurações da regra:

   a. No campo **Nome da regra**, insira ou edite 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**, 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. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

   d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

   e. 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.

   f. No campo **Escopo de uso 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.

      Somente o formato IPv4 é compatível com endereços IP.

   g. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

   h. Clique no botão **OK** para salvar a regra.

3. Na guia **Porta**, clique no botão **Adicionar**.

   A janela **Regra para portas** é aberta.

4. Defina as configurações da regra:

   a. No campo **Nome da regra**, insira ou edite o nome da regra.

   b. Na lista **Ação**, 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. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

   d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

e. No campo **Escopo de uso 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.

> Somente o formato IPv4 é compatível com endereços IP.

f. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

g. Clique no botão **OK** para salvar a regra.

5. Clique no botão **OK** na subseção **Regras para conexões de saída**.

8. Caso queira importar ou exportar as regras personalizadas de um arquivo XML, use o botão **Importar** ou **Exportar** no bloco **Importação e exportação das regras**.

9. Salvar alterações.

O Kaspersky Embedded Systems Security aplica as novas configurações. A data e hora nas quais as configurações foram alteradas são salvas no log de auditoria do sistema.

Criando e configurando regras de Firewall no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Na seção **Controle de atividades de rede**, clique no botão **Configurar** na subseção **Firewall**.

   A janela **Firewall** é aberta.

5. Defina o botão de alternância para **Firewall ATIVADO**.

6. No bloco **Conexões de entrada**, clique no botão **Configurar**.

   A janela **Regras para conexões de entrada** é aberta.

7. Crie e configure as regras do Firewall para as conexões de entrada.

   1. Na guia **Portas locais**, clique no botão **Adicionar**.

      A janela **Regra para portas** é aberta.

2. Defina as configurações da regra:

   a. No campo **Nome da regra**, insira ou edite o nome da regra.

   b. Na lista **Ação**, selecione uma das seguintes opções:

      - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de saída para as portas.
      - **Negar**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de saída para as portas.

   c. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

   d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

   e. No campo **Escopo de uso 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.

      Somente o formato IPv4 é compatível com endereços IP.

   f. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

   g. Clique no botão **OK** para salvar a regra.

3. Na guia **Aplicativos**, clique no botão **Adicionar**.

   A janela **Regra para aplicativos** é aberta.

4. Defina as configurações da regra:

   a. No campo **Nome da regra**, insira ou edite 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**, selecione uma das seguintes opções:

      - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de saída para o aplicativo.
      - **Negar**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de saída para o aplicativo.

   c. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

   d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

   e. No campo **Caminho do aplicativo**, especifique o caminho manualmente para o arquivo executável do aplicativo para o qual a regra está sendo configurada.

f. No campo **Escopo de uso 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.

> Somente o formato IPv4 é compatível com endereços IP.

g. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

h. Clique no botão **OK** para salvar a regra.

5. Clique no botão **OK** na subseção **Regras para conexões de entrada**.

8. No bloco **Conexões de saída**, clique no botão **Configurar**.

   A janela **Regras para conexões de saída** é aberta.

9. Crie e configure as regras do Firewall para as conexões de saída.

   1. Na guia **Portas locais**, clique no botão **Adicionar**.

      A janela **Regra para portas** é aberta.

   2. Defina as configurações da regra:

      a. No campo **Nome da regra**, insira ou edite o nome da regra.

      b. Na lista **Ação**, selecione uma das seguintes opções:

      - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de saída para as portas.
      - **Negar**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de saída para as portas.

      c. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

      d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

      e. No campo **Escopo de uso 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.

      > Somente o formato IPv4 é compatível com endereços IP.

      f. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

      g. Clique no botão **OK** para salvar a regra.

   3. Na guia **Aplicativos**, clique no botão **Adicionar**.

      A janela **Regra para aplicativos** é aberta.

4. Defina as configurações da regra:

   a. No campo **Nome da regra**, insira ou edite 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**, selecione uma das seguintes opções:

      - **Permitir**. Caso essa opção esteja selecionada, o aplicativo permitirá as conexões de rede de saída para o aplicativo.
      - **Negar**. Caso essa opção esteja selecionada, o aplicativo bloqueará as conexões de rede de saída para o aplicativo.

   c. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

   d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

   e. No campo **Caminho do aplicativo**, especifique o caminho manualmente para o arquivo executável do aplicativo para o qual a regra está sendo configurada.

   f. No campo **Escopo de uso 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.

      Somente o formato IPv4 é compatível com endereços IP.

   g. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

   h. Clique no botão **OK** para salvar a regra.

5. Clique no botão **OK** na subseção **Regras para conexões de saída**.

10. Caso queira importar ou exportar as regras personalizadas de um arquivo XML, use o botão **Importação de regras** ou **Exportação de regras** no bloco **Importação e exportação das regras**.

11. Salvar alterações.

O Kaspersky Embedded Systems Security aplica as novas configurações. A data e hora nas quais as configurações foram alteradas são salvas no log de auditoria do sistema.

Criando e configurando as regras de Firewall no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Firewall**.
2. no painel de resultados do node **Firewall**, clique no link **Propriedades**.

   A janela **Propriedades: Firewall** é aberta.
3. No bloco **Conexões de entrada**, clique no botão **Lista de regras**.

   A janela **Regras para conexões de entrada** é aberta.
4. Crie e configure as regras do Firewall para as conexões de entrada.

   1. Na guia **Aplicativos**, clique no botão **Adicionar**.

      A janela **Regra para um aplicativo** é aberta.
   2. Defina as configurações da regra:

      a. No campo **Nome da regra**, insira ou edite 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**, 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. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

      d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

      e. 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.

      f. No campo **Escopo de uso 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.

      > Somente o formato IPv4 é compatível com endereços IP.

      g. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

      h. Clique no botão **OK** para salvar a regra.

3. Na guia **Portas locais**, clique no botão **Adicionar**.

   A janela **Regra para portas** é aberta.

4. Defina as configurações da regra:

   a. No campo **Nome da regra**, insira ou edite o nome da regra.

   b. Na lista **Ação**, 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. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

   d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

   e. No campo **Escopo de uso 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.

   > Somente o formato IPv4 é compatível com endereços IP.

   f. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

   g. Clique no botão **OK** para salvar a regra.

5. Clique no botão **OK** na subseção **Regras para conexões de entrada**.

5. No bloco **Conexões de saída**, clique no botão **Lista de regras**.

   A janela **Regras para conexões de saída** é aberta.

6. **Crie e configure as regras do Firewall para as conexões de saída**.

   1. Na guia **Aplicativos**, clique no botão **Adicionar**.

      A janela **Regra para um aplicativo** é aberta.

   2. Defina as configurações da regra:

      a. No campo **Nome da regra**, insira ou edite 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**, 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. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

e. 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.

f. No campo **Escopo de uso 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.

> Somente o formato IPv4 é compatível com endereços IP.

g. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

h. Clique no botão **OK** para salvar a regra.

3. Na guia **Porta**, clique no botão **Adicionar**.

   A janela **Regra para portas** é aberta.

4. Defina as configurações da regra:

a. No campo **Nome da regra**, insira ou edite o nome da regra.

b. Na lista **Ação**, 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. Marque a caixa de seleção **Protocolo** para selecionar o tipo de protocolo para o qual o aplicativo controlará as conexões de rede de entrada.

d. Nos blocos **Portas locais** e **Portas remotas**, especifique uma porta ou um intervalo de portas.

e. No campo **Escopo de uso 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.

> Somente o formato IPv4 é compatível com endereços IP.

f. No bloco **Adaptadores de rede**, especifique a lista de adaptadores de rede.

g. Clique no botão **OK** para salvar a regra.

5. Clique no botão **OK** na subseção **Regras para conexões de saída**.

7. Caso queira importar ou exportar as regras personalizadas de um arquivo XML, use o botão **Importar** ou **Exportar** no bloco **Importação e exportação das regras**.

8. Para importar regras do Firewall do Windows, clique em **Importar regras do Firewall do Windows**.

Em computadores Windows 11 24H2, o aplicativo pode ignorar determinadas regras do Firewall do Windows. Devido aos recursos especiais desta versão do sistema operacional, talvez o Kaspersky Embedded Systems Security não reconheça os parâmetros de algumas regras para pacotes do aplicativo.

9. Salvar alterações.

O Kaspersky Embedded Systems Security aplica as novas configurações. 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

Criando e configurando regras de Firewall no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na seção **Controle de atividades de rede**, clique no botão **Configurações** na subseção **Firewall**.
   A janela **Firewall** é aberta.

4. Na janela aberta, clique no botão **Lista de regras** na seção **Conexões de entrada** ou **Conexões de saída**, dependendo do tipo de regra para o qual se deseja alterar o status.

5. Na janela que é aberta, selecione a guia **Aplicativos** ou **Portas locais** .
   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. Para excluir as regras da lista, selecione as regras e clique em **Excluir**.
7. Salvar alterações.

Criando e configurando regras de Firewall no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Na seção **Controle de atividades de rede**, clique no botão **Configurar** na subseção **Firewall**.

   A janela **Firewall** é aberta.
5. Na janela aberta, clique no botão **Configurar** na seção **Conexões de entrada** ou **Conexões de saída**, dependendo do tipo de regra para o qual se deseja alterar o status.
6. Na janela que é aberta, selecione a guia **Portas locais** ou **Aplicativos** .

   Na lista de regras, selecione a regra cujo status você deseja modificar e execute uma das seguintes ações:

   - Se você quiser ativar uma regra desativada, marque a caixa de seleção à esquerda do nome da regra.

     A regra selecionada será ativada.
   - Se você quiser desativar uma regra ativada, desmarque a caixa de seleção à esquerda do nome da regra.

     A regra selecionada será desativada.
7. Para excluir as regras da lista, selecione as regras e clique em **Excluir**.
8. Salvar alterações.

Criando e configurando as regras de Firewall no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Controle do Computador** → **Firewall**.
2. no painel de resultados do node **Firewall**, clique no link **Propriedades**.

   A janela **Propriedades: Firewall** é aberta.
3. Na janela aberta, clique no botão **Lista de regras** na seção **Conexões de entrada** ou **Conexões de saída**, dependendo do tipo de regra para o qual se deseja alterar o status.
4. Na janela que é aberta, selecione a guia **Aplicativos** ou **Portas locais** .

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.

5. Para excluir as regras da lista, selecione as regras e clique em **Excluir**.

6. Salvar alterações.

Prevenção contra ataque BadUSB

O componente de Proteção contra ataque BadUSB não está instalado por padrão. É possível adicionar um componente durante a instalação do aplicativo ou alterar o conjunto de componentes do aplicativo após a instalação do aplicativo.

Alguns vírus modificam o firmware dos dispositivos USB para enganar o sistema operacional em detectar o dispositivo USB como um teclado. Como resultado, o vírus pode executar comandos em sua conta de usuário para baixar malware, por exemplo.

O componente Prevenção contra ataque BadUSB previne dispositivos de USB infectados que emulam um teclado de unir-se ao computador.

Quando um dispositivo USB é conectado ao computador e identificado pelo sistema operacional como um teclado, o aplicativo solicita que o usuário insira um código numérico gerado pelo aplicativo nesse teclado ou usando um teclado virtual caso disponível. Esse procedimento é conhecido como autorização do teclado.

Se o código tiver sido inserido corretamente, o aplicativo salvará os parâmetros de identificação – VID/PID do teclado e o número da porta à qual ele foi conectado – na lista de teclados autorizados. A autorização do teclado não precisa ser repetida quando o teclado for reconectado ou após o sistema operacional ser reiniciado.

Quando o teclado autorizado é conectado à uma porta USB diferente do computador, o aplicativo exibe uma solicitação para autorização desse teclado novamente.

Se o código numérico tiver sido inserido de forma incorreta, o aplicativo gerará um novo código. É possível configurar o número de tentativas para inserção do código numérico. Caso o código numérico seja inserido incorretamente várias vezes ou a janela de autorização do teclado seja fechada, o aplicativo bloqueia a entrada pelo teclado. Quando o tempo de bloqueio do dispositivo USB termina ou o sistema operacional é reiniciado, o aplicativo solicita ao usuário a autorização do teclado novamente.

O aplicativo permite a utilização de um teclado autorizado e bloqueia um teclado que não tenha sido autorizado.

Os dispositivos USB identificados pelo sistema operacional como teclados e conectados ao computador antes da instalação do componente Prevenção contra ataque BadUSB são considerados autorizados após instalação do componente.

Como ativar e configurar o componente Prevenção Contra Ataque BadUSB no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de propriedades da política, acesse a seção **Controle de atividades locais**.
4. No bloco **Prevenção contra ataque BadUSB**, clique no botão **Configurações**.
   A janela **Prevenção contra ataque BadUSB** é aberta.

5. Use a caixa de seleção **Prevenção contra ataque BadUSB** para ativar ou desativar o componente.

6. Na seção **Autorização de dispositivos USB**, defina as seguintes configurações:

   - **Número máximo de tentativas de autorização do dispositivo USB**. Bloquear automaticamente o dispositivo USB caso o código de autorização seja inserido incorretamente o número especificado de vezes. Os valores válidos são de 1 a 10. Por exemplo, caso permita 5 tentativas de inserção do código de autorização, o dispositivo USB será bloqueado após a quinta tentativa falhada. O Kaspersky Embedded Systems Security exibe a duração do bloqueio do dispositivo USB. Após esse tempo, é possível ter 5 tentativas para inserção do código de autorização.

   - **Tempo limite ao atingir o número máximo de tentativas (minutos)**. Duração do bloqueio do dispositivo USB após o número especificado de tentativas malsucedidas de inserção do código de autorização. Os valores válidos são de 1 a 180 (minutos).

7. Na seção **Autorização do dispositivo USB após conexão**, defina as seguintes configurações:

   - **Proibir o uso do Teclado na tela para a autorização de dispositivos USB**. Caso a caixa de seleção seja marcada, o aplicativo proibirá o uso do teclado na tela para a autorização de dispositivos USB do qual um código de autorização não pode ser inserido (por exemplo, scanners de código de barras).

   - **Proibir o uso do código de barras para autorização de dispositivos USB**. Caso a caixa de seleção seja marcada, o aplicativo não exibirá o código de barras na notificação de autorização do leitor de código de barras.

8. Feche os cadeados para aplicar a política aos computadores.

9. Clique no botão **OK** para salvar as alterações.

Como ativar e configurar o componente Prevenção Contra Ataque BadUSB no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Selecione a seção **Controle de atividades locais**.

5. No bloco **Prevenção contra ataque BadUSB**, clique no botão **Configurar**.

   A janela **Prevenção contra ataque BadUSB** é aberta.

6. Use o botão de alternância do **Prevenção contra ataque BadUSB** para ativar ou desativar o componente.

7. Ative ou desative o botão de alternância **Proibir o uso do Teclado na tela para autorização de dispositivos USB ATIVADO** para permitir ou bloquear o uso do Teclado na tela para autorização de dispositivos USB aos quais um código de autorização não pode ser inserido (por exemplo, scanners de código de barras).

8. Ative ou desative a botão de alternância **Proibir o uso do código de barras para autorização de dispositivos USB ATIVADO** para permitir ou bloquear a exibição de um código de barras na notificação para autorização do leitor de código de barras.

9. Na seção **Autorização de dispositivos USB**, defina as seguintes configurações:

   - **Número máximo de tentativas de autorização do dispositivo USB (1-10)**. Bloquear automaticamente o dispositivo USB caso o código de autorização seja inserido incorretamente o número especificado de vezes. Os valores válidos são de 1 a 10. Por exemplo, caso permita 5 tentativas de inserção do código de autorização, o dispositivo USB será bloqueado após a quinta tentativa falhada. O Kaspersky Embedded Systems Security exibe a duração do bloqueio do dispositivo USB. Após esse tempo, é possível ter 5 tentativas para inserção do código de autorização.

   - **Tempo limite ao atingir o número máximo de tentativas em minutos (1-180)**. Duração do bloqueio do dispositivo USB após o número especificado de tentativas malsucedidas de inserção do código de autorização. Os valores válidos são de 1 a 180 (minutos).

10. Feche os cadeados para aplicar a política aos computadores.

11. Clique no botão **OK** para salvar as alterações.

Como ativar e configurar o componente Prevenção Contra Ataque BadUSB no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o node **Controle do Computador → Prevenção contra ataque BadUSB**.

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

   A janela **Prevenção contra ataque BadUSB** é aberta.

3. Use a caixa de seleção **Prevenção contra ataque BadUSB** para ativar ou desativar o componente.

4. Na seção **Autorização de dispositivos USB**, defina as seguintes configurações:

   - **Número máximo de tentativas de autorização do dispositivo USB**. Bloquear automaticamente o dispositivo USB caso o código de autorização seja inserido incorretamente o número especificado de vezes. Os valores válidos são de 1 a 10. Por exemplo, caso permita 5 tentativas de inserção do código de autorização, o dispositivo USB será bloqueado após a quinta tentativa falhada. O Kaspersky Embedded Systems Security exibe a duração do bloqueio do dispositivo USB. Após esse tempo, é possível ter 5 tentativas para inserção do código de autorização.

   - **Tempo limite ao atingir o número máximo de tentativas (minutos)**. Duração do bloqueio do dispositivo USB após o número especificado de tentativas malsucedidas de inserção do código de autorização. Os valores válidos são de 1 a 180 (minutos).

5. Na seção **Autorização do dispositivo USB após conexão**, defina as seguintes configurações:

- **Proibir o uso do Teclado na tela para a autorização de dispositivos USB**. Caso a caixa de seleção seja marcada, o aplicativo proibirá o uso do teclado na tela para a autorização de dispositivos USB do qual um código de autorização não pode ser inserido (por exemplo, scanners de código de barras).

- **Proibir o uso do código de barras para autorização de dispositivos USB**. Caso a caixa de seleção seja marcada, o aplicativo não exibirá o código de barras na notificação de autorização do leitor de código de barras.

6. Clique no botão **OK** para salvar as alterações.

Monitor de integridade do sistema

Agora, o Kaspersky Embedded Systems Security 4.0 inclui o componente monitor de integridade do sistema em vez do componente Monitor de Integridade de Arquivos. O componente monitor de integridade do sistema inclui todas as funcionalidades do monitor de integridade de arquivos. Além disso, ele permite monitorar as alterações do registro e a conexão de dispositivos externos.

O componente monitor de integridade do sistema monitora as alterações no sistema operacional que podem indicar violações de segurança do computador. Quando essas alterações são detectadas, o Kaspersky Embedded Systems Security gera os eventos correspondentes e alerta o administrador. O monitor de integridade do sistema pode operar no modo em tempo real e também pode executar verificações de integridade do sistema sob demanda.

Monitor de integridade do sistema em tempo real

No modo em tempo real, o monitor de integridade do sistema rastreia as alterações nos objetos incluídos no escopo do componente (o escopo de monitoramento). O monitor de integridade do sistema também permite bloquear o acesso não autorizado a esses objetos em tempo real.

Verificação de integridade do sistema sob demanda

A verificação de integridade do sistema sob demanda é uma tarefa que pode ser manualmente executada ou por agendamento. Para executar a tarefa **Monitor de integridade do sistema de linha de base**, é necessário configurar o escopo do componente (o escopo de monitoramento) e criar uma linha de base. A linha de base é um estado registrado de objetos no sistema que o aplicativo usa como referência ao comparar com o estado atual. Uma linha de base é criada quando a tarefa é iniciada pela primeira vez.

Migração das configurações do Monitor de integridade de arquivos

Ao atualizar o Kaspersky Embedded Systems Security para a versão 3.4 ou anterior à versão 4.0, o Monitor de Integridade de Arquivos e as configurações do Monitor de Acesso ao Registro são migrados automaticamente. Como parte da migração, o aplicativo move as regras de monitoramento para o monitor de integridade do sistema.

Sobre as regras do monitor de integridade do sistema

Para que o monitor de integridade do sistema funcione, é necessário adicionar pelo menos uma regra. A *regra do monitor de integridade do sistema* é um conjunto de critérios que definem o acesso dos usuários aos arquivos ou ao registro. O monitor de integridade do sistema detecta alterações nos arquivos ou no registro dentro do *escopo de monitoramento*. O escopo de monitoramento é um dos critérios de uma regra do monitor de integridade do sistema.

O monitor de integridade do sistema permite monitorar os seguintes objetos:

- Arquivos
- Registro
- Dispositivos externos

Considerações especiais envolvidas no monitoramento de arquivos

O monitor de integridade do sistema monitora as alterações em arquivos e pastas, além dos arquivos que estão sendo adicionados ao escopo de monitoramento ou removidos dele. Essas alterações podem indicar uma violação da segurança do computador. Recomendamos adicionar objetos raramente modificados ou objetos aos quais apenas o administrador tem acesso. Isso reduzirá o número de eventos do monitor de integridade do sistema.

O Kaspersky Embedded Systems Security monitora as alterações de arquivos e pastas somente nos discos que estavam conectados quando o monitor de integridade do sistema em tempo real começou a funcionar. Se um disco não estivesse conectado quando o monitor de integridade do sistema em tempo real tivesse começado a operar, o aplicativo não monitoraria as alterações de arquivos e pastas nesse disco, mesmo se os arquivos e pastas fossem adicionados ao escopo de monitoramento.

Considerações especiais envolvidas no monitoramento do registro

O monitor de integridade do sistema monitora o registro. Essas alterações podem indicar uma violação da segurança do computador.

O monitor de integridade do sistema monitora as seguintes chaves raiz do registro:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG`.

O monitor de integridade do sistema não é compatível com a chave `HKEY_CURRENT_USER`. É possível especificar uma chave em `HKEY_USERS` como `HKEY_USERS\<user profile ID>\<key>`.

Considerações especiais envolvidas no monitoramento de dispositivos externos

O monitor de integridade do sistema monitora a conexão e desconexão de dispositivos externos. O procedimento é necessário para proteger o computador contra as ameaças de segurança do possível resultado da troca de arquivos com esses dispositivos. O monitor de integridade do sistema não monitora o acesso aos dispositivos externos e não bloqueia a troca de arquivos. É possível configurar o acesso aos dispositivos com o uso de um componente de aplicativo diferente, o Controle de dispositivos.

Ao executar a tarefa *Monitor de integridade do sistema de linha de base*, o aplicativo ignorará a reconexão de dispositivos externos se os dispositivos tiverem a mesma letra de unidade no sistema operacional. Para que sejam registrados em log, os dispositivos reconectados devem ter letras de unidade diferentes.

O monitor de integridade do sistema monitora a conexão dos seguintes tipos de dispositivos externos:

- Unidade removível (incluindo unidades flash USB)
- Disco rígido.
- Adaptador de rede externo.
- Unidade de CD/DVD/Blu-ray.
- Scanner / câmera.

Monitor de integridade do sistema em tempo real

O monitor de integridade do sistema permite rastrear alterações no sistema operacional em tempo real. É possível rastrear as alterações que podem indicar violações de segurança no computador. O componente permite bloquear essas alterações ou simplesmente registrar os eventos de alteração.

Para que o monitor de integridade do sistema funcione, é necessário adicionar pelo menos uma regra. A regra do monitor de integridade do sistema é um conjunto de critérios que definem o acesso dos usuários aos arquivos e ao registro. O monitor de integridade do sistema detecta alterações nos arquivos e no registro dentro do escopo de monitoramento. O escopo de monitoramento é um dos critérios de uma regra do monitor de integridade do sistema.

Como ativar e configurar o monitor de integridade do sistema em tempo real no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Inspeção do sistema**.
4. Na seção **Monitor de integridade do sistema**, clique no botão **Configurações**.
5. Marque a caixa de seleção **Monitor de integridade do sistema**.
6. Configure a tarefa de Monitor de Integridade de Arquivos:
   a. Marque a caixa de seleção **Monitorar arquivos** na guia **Arquivos**.
   b. Abaixo de **Modo de operação para regras de bloqueio**, selecione um modo do monitor de integridade do arquivo:
      - **Bloquear**. Nesse modo, o aplicativo executa ações nos arquivos de acordo com as regras do monitor de integridade de arquivos e gera os eventos correspondentes no log do monitor de integridade do sistema.
      - **Informar**. Nesse modo, o aplicativo gera somente os eventos sobre as regras acionadas do monitor de integridade de arquivos no log do monitor de integridade do sistema.

c. Adicione as regras do Monitor de Integridade de Arquivos de forma manual usando o botão **Adicionar** ou importando de um arquivo XML. As configurações da regra do Monitor de Integridade de Arquivos estão descritas na seguinte tabela.

d. Na lista de regras do Monitor de Integridade de Arquivos, gerencie as caixas de seleção para deixar as regras necessárias ativadas.

7. Configure o Monitor de Acesso ao Registro:

a. Marque a caixa de seleção **Monitorar o registro** na guia **Registro**.

b. Em **Modo de operação para regras de bloqueio**, selecione um modo para o Monitor de Acesso ao Registro:

- **Bloquear**. Nesse modo, o aplicativo bloqueia as ações com o registro de acordo com as regras do Monitor de Acesso ao Registro e gera eventos correspondentes no log do monitor de integridade do sistema.
- **Informar**. Nesse modo, o aplicativo gera somente os eventos sobre as regras acionadas do monitor de acesso do registro no log do monitor de integridade do sistema.

c. Adicione as regras do Monitor de Acesso ao Registro de forma manual usando o botão **Adicionar** ou importando de um arquivo XML. As configurações da regra do Monitor de Acesso ao Registro estão descritas na seguinte tabela.

d. Na lista de regras do Monitor de Acesso ao Registro, gerencie as caixas de seleção para deixar as regras necessárias ativadas.

8. Configure o monitoramento de dispositivos externos:

a. Marque a caixa de seleção **Monitorar dispositivos** na guia **Dispositivos**.

b. Na lista suspensa **Nível de gravidade do evento**, selecione o nível de importância dos eventos de monitoramento de dispositivos externos: *Informativo*, *Aviso*, *Crítico*.

Depois de aplicar as configurações de monitoramento do dispositivo externo, o aplicativo lembrará as conexões atuais do dispositivo externo. Depois, quando um dispositivo externo é conectado ou desconectado, o aplicativo gera um evento correspondente no log do monitor de integridade do sistema.

9. Salvar alterações.

Como ativar e configurar o monitor de integridade do sistema em tempo real no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Inspeção do sistema** → **Monitor de integridade do sistema** e clique no botão **Configurar**.

5. Marque a caixa de seleção **Monitor de integridade do sistema**.

6. Configure a tarefa de Monitor de Integridade de Arquivos:

   a. Marque a caixa de seleção **Monitorar arquivos** na guia **Arquivos**.

   b. Abaixo de **Modo de operação para regras de bloqueio**, selecione um modo do monitor de integridade do arquivo:

      - **Bloquear**. Nesse modo, o aplicativo executa ações nos arquivos de acordo com as regras do monitor de integridade de arquivos e gera os eventos correspondentes no log do monitor de integridade do sistema.

      - **Informar**. Nesse modo, o aplicativo gera somente os eventos sobre as regras acionadas do monitor de integridade de arquivos no log do monitor de integridade do sistema.

   c. Adicione as regras do Monitor de Integridade de Arquivos de forma manual usando o botão **Adicionar** ou importando de um arquivo XML. As configurações da regra do Monitor de Integridade de Arquivos estão descritas na seguinte tabela.

   d. Na lista de regras do Monitor de Integridade de Arquivos, gerencie as caixas de seleção na coluna **Status** para deixar as regras necessárias ativadas.

7. Configure o Monitor de Acesso ao Registro:

   a. Marque a caixa de seleção **Monitorar o registro** na guia **Registro**.

   b. Em **Modo de operação para regras de bloqueio**, selecione um modo para o Monitor de Acesso ao Registro:

      - **Bloquear**. Nesse modo, o aplicativo bloqueia as ações com o registro de acordo com as regras do Monitor de Acesso ao Registro e gera eventos correspondentes no log do monitor de integridade do sistema.

      - **Informar**. Nesse modo, o aplicativo gera somente os eventos sobre as regras acionadas do monitor de acesso do registro no log do monitor de integridade do sistema.

   c. Adicione as regras do Monitor de Acesso ao Registro de forma manual usando o botão **Adicionar** ou importando de um arquivo XML. As configurações da regra do Monitor de Acesso ao Registro estão descritas na seguinte tabela.

   d. Na lista de regras do Monitor de Acesso ao Registro, gerencie as caixas de seleção na coluna **Status** para deixar as regras necessárias ativadas.

8. Configure o monitoramento de dispositivos externos:

   a. Marque a caixa de seleção **Monitorar dispositivos** na guia **Dispositivos**.

   b. Na lista suspensa **Nível de gravidade do evento**, selecione o nível de importância dos eventos de monitoramento de dispositivos externos: *Informativo*, *Aviso*, *Crítico*.

      O monitor de integridade do sistema registra a conexão atual dos dispositivos externos. O aplicativo começa a monitorar a conexão e desconexão dos dispositivos externos depois que o componente é ativado nas configurações do aplicativo. Depois, quando um dispositivo externo é conectado ou desconectado, o aplicativo gera um evento correspondente.

9. Salvar alterações.

Como ativar e configurar o monitor de integridade do sistema em tempo real no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Inspeção do sistema** → **Monitor de integridade do sistema**.
2. no painel de resultados do node **Monitor de integridade do sistema**, clique no link **Propriedades**.

   A janela **Propriedades: Monitor de integridade do sistema** é aberta.
3. Marque a caixa de seleção **Monitor de integridade do sistema**.
4. Configure a tarefa de Monitor de Integridade de Arquivos:
   a. Marque a caixa de seleção **Monitorar arquivos** na guia **Arquivos**.
   b. Abaixo de **Modo de operação para regras de bloqueio**, selecione um modo do monitor de integridade do arquivo:
      - **Bloquear**. Nesse modo, o aplicativo executa ações nos arquivos de acordo com as regras do monitor de integridade de arquivos e gera os eventos correspondentes no log do monitor de integridade do sistema.
      - **Informar**. Nesse modo, o aplicativo gera somente os eventos sobre as regras acionadas do monitor de integridade de arquivos no log do monitor de integridade do sistema.
   c. Adicione as regras do Monitor de Integridade de Arquivos de forma manual usando o botão **Adicionar** ou importando de um arquivo XML. As configurações da regra do Monitor de Integridade de Arquivos estão descritas na seguinte tabela.
   d. Na lista de regras do Monitor de Integridade de Arquivos, gerencie as caixas de seleção para deixar as regras necessárias ativadas.
5. Configure o Monitor de Acesso ao Registro:
   a. Marque a caixa de seleção **Monitorar o registro** na guia **Registro**.
   b. Em **Modo de operação para regras de bloqueio**, selecione um modo para o Monitor de Acesso ao Registro:
      - **Bloquear**. Nesse modo, o aplicativo bloqueia as ações com o registro de acordo com as regras do Monitor de Acesso ao Registro e gera eventos correspondentes no log do monitor de integridade do sistema.
      - **Informar**. Nesse modo, o aplicativo gera somente os eventos sobre as regras acionadas do monitor de acesso do registro no log do monitor de integridade do sistema.
   c. Adicione as regras do Monitor de Acesso ao Registro de forma manual usando o botão **Adicionar** ou importando de um arquivo XML. As configurações da regra do Monitor de Acesso ao Registro estão descritas na seguinte tabela.
   d. Na lista de regras do Monitor de Acesso ao Registro, gerencie as caixas de seleção para deixar as regras necessárias ativadas.

6. Configure o monitoramento de dispositivos externos:

   a. Marque a caixa de seleção **Monitorar dispositivos** na guia **Dispositivos**.

   b. Na lista suspensa **Nível de gravidade do evento**, selecione o nível de importância dos eventos de monitoramento de dispositivos externos: *Informativo*, *Aviso* e *Crítico*.

      Depois de aplicar as configurações de monitoramento do dispositivo externo, o aplicativo lembrará as conexões atuais do dispositivo externo. Depois, quando um dispositivo externo é conectado ou desconectado, o aplicativo gera um evento correspondente no log do monitor de integridade do sistema.

7. Salvar alterações.

Configurações das regras do monitor de integridade do sistema

Parâmetro	Descrição
Monitorar operações de arquivos para o escopo	O escopo ao qual se deseja aplicar o Monitor de Integridade de Arquivos. Esse campo é obrigatório. Usar máscaras: O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara: O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas. Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida. O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres \ e / (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.
Objetos monitorados	Aqui é possível especificar o nome ou o valor de uma chave de registro. Usar máscaras: O Kaspersky Embedded Systems Security é compatível com os caracteres `*` e `?` ao inserir uma máscara:
Operações com arquivos	• **Detectar**. O aplicativo permite executar ações em arquivos no escopo de monitoramento. • **Detectar e bloquear**. O que o aplicativo faz depende do modo do Monitor de Integridade de Arquivos selecionado. Caso o modo *Bloquear* seja selecionado, o monitor de integridade do sistema bloqueará a execução de ações com os arquivos do escopo de monitoramento. Caso o modo *Informar* seja selecionado, o monitor de integridade do sistema permitirá executar ações com os arquivos do escopo de monitoramento.
Usuários e/ou grupos de usuários confiáveis	Um usuário confiável é um usuário com permissão para executar ações com os arquivos e chaves do registro no escopo de monitoramento. Caso o Kaspersky Embedded Systems Security detecte uma ação executada por um usuário confiável, o monitor de integridade do sistema gerará um evento Informativo . É possível selecionar usuários no Active Directory, na lista de contas no Kaspersky Security Center ou ao inserir um nome de usuário local manualmente.
Marcadores de operação de arquivo / Ações	Marcadores que caracterizam a ação com os arquivos ou chaves de registro que serão monitorados pelo aplicativo.
Detectar as operações de arquivo de acordo com todos os marcadores reconhecidos / Detectar as operações de registro de acordo com todos os marcadores reconhecidos	Por padrão, o Kaspersky Embedded Systems Security detecta todos os marcadores de operações de arquivos / registro.
Detectar operações de arquivo com base nos seguintes marcadores / Detectar as operações de registro de acordo com os seguintes marcadores	Na lista de operações de arquivos / registro disponíveis, selecione as caixas ao lado das operações que deseja monitorar.

Parâmetro	Descrição
Calcular um checksum após uma operação do arquivo, se possível. O checksum será indicado no log da tarefa	Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security calculará a soma de verificação do arquivo modificado, se uma operação de arquivo com pelo menos um marcador selecionado tiver sido detectada. Caso a operação de arquivo seja detectada por diversos marcadores, apenas a soma de verificação do arquivo final, após todas as modificações, será calculada. Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security não calculará a soma de verificação de arquivos modificados. Nenhum cálculo da soma de verificação será realizado nos casos a seguir: • Se o arquivo tiver ficado indisponível (por exemplo, devido à modificação de permissões de acesso). • Se a operação de arquivo for detectada em um arquivo que foi removido posteriormente. Por padrão, a caixa de seleção fica desmarcada.
Algoritmo de computação de soma de verificação	Selecione um dos algoritmos de cálculo de soma de verificação na lista suspensa: • Hash MD5 • Hash SHA256
Exclusões	Na guia **Exclusões**, é possível adicionar os objetos que se deseja excluir do escopo de monitoramento: • Para uma regra do Monitor de Integridade de Arquivos, é possível especificar uma lista de pastas. • Para uma regra do monitor de acesso ao registro, é possível especificar chaves ou valores de registro. Usar máscaras: **Arquivos** Lista de arquivos e pastas monitorados pelo componente. O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara: O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas. Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida. O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres. **Registro** O Kaspersky Embedded Systems Security tem suporte para os caracteres `*` e `?` ao inserir uma máscara: as entradas de exclusão têm uma prioridade mais alta do que as entradas do escopo de monitoramento.
Nível de gravidade do evento	O Kaspersky Embedded Systems Security registra eventos de modificação de arquivo sempre que um arquivo de registro no escopo de monitoramento é modificado. Estão disponíveis os seguintes níveis de gravidade do evento: **Informativo**, **Aviso**, **Crítico**.

Verificação de integridade do sistema sob demanda

A verificação de integridade do sistema sob demanda é uma tarefa que pode ser manualmente executada ou por agendamento. Ao executar a tarefa *Monitor de integridade do sistema de linha de base*, o aplicativo compara o estado atual dos objetos incluídos no escopo de monitoramento com seu estado de *linha de base*. Uma linha de base é criada quando a tarefa é iniciada pela primeira vez.

Para que o monitor de integridade do sistema funcione, é necessário adicionar pelo menos uma regra. A regra do monitor de integridade do sistema é um conjunto de critérios que definem o acesso dos usuários aos arquivos e ao registro. O monitor de integridade do sistema detecta alterações nos arquivos e no registro dentro do escopo de monitoramento. O escopo de monitoramento é um dos critérios de uma regra do monitor de integridade do sistema.

Configuração do escopo de monitoramento para a tarefa Monitor de integridade do sistema de linha de base

Por padrão, o escopo de monitoramento da tarefa *Monitor de integridade do sistema de linha de base* é igual ao escopo de monitoramento do monitor de integridade do sistema. É possível configurar um escopo de monitoramento diferente para a tarefa.

O Monitor de integridade do sistema não é compatível com a importação de chaves `HKEY_CURRENT_USER` e `HKEY_CURRENT_CONFIG` para a tarefa *Verificação de integridade do sistema*. Caso o escopo de monitoramento da tarefa contenha essas chaves, o aplicativo gerará o evento *O escopo de monitoramento inclui objetos incorretos*.

Como configurar um escopo de monitoramento diferente para a tarefa Monitor de integridade do sistema de linha de base no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Tarefas**.
2. Selecione a tarefa *Monitor de integridade do sistema de linha de base* necessária e clique duas vezes para abrir as propriedades dela.
3. Na janela aberta, selecione **Configurações**.
4. Configurar o monitoramento de arquivo:
    a. Marque a caixa de seleção **Monitorar arquivos** na guia **Arquivos**.
    b. Selecione as regras na lista ao marcar as caixas de seleção.
    c. Caso seja necessário, adicione uma nova regra clicando no botão **Adicionar**. As configurações de regra do Monitor de integridade do sistema de linha de base estão descritas na seguinte tabela.
    d. Também é possível importar as regras de outra fonte.
5. Configurar o monitoramento do registro:
    a. Marque a caixa de seleção **Monitorar o registro** na guia **Registro**.
    b. Selecione as regras na lista ao marcar as caixas de seleção.
    c. Caso seja necessário, adicione uma nova regra clicando no botão **Adicionar**. As configurações de regra do Monitor de integridade do sistema de linha de base estão descritas na seguinte tabela.
    d. Também é possível importar as regras de outra fonte.

6. Configure o monitoramento de dispositivos externos:

    a. Marque a caixa de seleção **Monitorar dispositivos** na guia **Dispositivos**.

    b. Na lista suspensa **Nível de gravidade do evento**, selecione o nível de importância dos eventos de monitoramento de dispositivos externos: *Informativo*, *Aviso*, *Crítico*.

    O monitor de integridade do sistema registra informações sobre dispositivos externos conectados no momento em que a linha de base é criada. Subsequentemente, quando um dispositivo externo é conectado, o aplicativo gera um evento correspondente. Ao executar a tarefa, o aplicativo não monitora a desconexão dos dispositivos externos.

7. Salvar alterações.

Como configurar um escopo de monitoramento diferente para a tarefa Monitor de integridade do sistema de linha de base no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Tarefas**.

2. Selecione a tarefa *Monitor de integridade do sistema de linha de base* necessária e clique duas vezes para abrir as propriedades dela.

3. Na janela aberta, selecione **Configurações do aplicativo**.

4. Configurar o monitoramento de arquivo:

    a. Marque a caixa de seleção **Monitorar arquivos**.

    b. Selecione as regras na lista ao marcar as caixas de seleção.

    c. Caso seja necessário, adicione uma nova regra clicando no botão **Adicionar**. As configurações de regra do Monitor de integridade do sistema de linha de base estão descritas na seguinte tabela.

    d. Também é possível importar as regras de outra fonte.

5. Configurar o monitoramento do registro:

    a. Marque a caixa de seleção **Monitorar o registro**.

    b. Selecione as regras na lista ao marcar as caixas de seleção.

    c. Caso seja necessário, adicione uma nova regra clicando no botão **Adicionar**. As configurações de regra do Monitor de integridade do sistema de linha de base estão descritas na seguinte tabela.

    d. Também é possível importar as regras de outra fonte.

6. Configure o monitoramento de dispositivos externos:

    a. Marque a caixa de seleção **Monitorar dispositivos**.

    b. Na lista suspensa **Nível de gravidade do evento**, selecione o nível de importância dos eventos de monitoramento de dispositivos externos: *Informativo*, *Aviso!* e *Crítico*.

    A tarefa *Monitor de integridade do sistema de linha de base* registra informações sobre dispositivos externos conectados no momento em que a linha de base é criada. Subsequentemente, quando um dispositivo externo é conectado, o aplicativo gera um evento correspondente. Ao executar a tarefa, o aplicativo não monitora a desconexão dos dispositivos externos.

7. Salvar alterações.

Como configurar um escopo de monitoramento diferente para a tarefa Monitor de integridade do sistema de linha de base no Console do Aplicativo

As propriedades da tarefa **Monitor de integridade do sistema de linha de base** são editáveis no Kaspersky Embedded Systems Security Console caso a tarefa tenha sido criada localmente ou caso a caixa de seleção **Permitir uso de tarefas locais** seja marcada na seção **Configurações do aplicativo → Executar as tarefas do sistema local** das propriedades da política.

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Inspeção do sistema → Monitor de integridade do sistema de linha de base**.

2. no painel de resultados do node **Monitor de integridade do sistema de linha de base**, clique no link **Propriedades**.

    A janela **Propriedades: Monitor de integridade do sistema de linha de base** é aberta.

3. Configurar o monitoramento de arquivo:

    a. Marque a caixa de seleção **Monitorar arquivos** na guia **Arquivos**.

    b. Selecione as regras na lista ao marcar as caixas de seleção.

    c. Caso seja necessário, adicione uma nova regra clicando no botão **Adicionar**. As configurações de regra do Monitor de integridade do sistema de linha de base estão descritas na seguinte tabela.

    d. Também é possível importar as regras de outra fonte.

4. Configurar o monitoramento do registro:

    a. Marque a caixa de seleção **Monitorar o registro** na guia **Registro**.

    b. Selecione as regras na lista ao marcar as caixas de seleção.

    c. Caso seja necessário, adicione uma nova regra clicando no botão **Adicionar**. As configurações de regra do Monitor de integridade do sistema de linha de base estão descritas na seguinte tabela.

    d. Também é possível importar as regras de outra fonte.

5. Configure o monitoramento de dispositivos externos:

   a. Marque a caixa de seleção **Monitorar dispositivos** na guia **Dispositivos**.

   b. Na lista suspensa **Nível de gravidade do evento**, selecione o nível de importância dos eventos de monitoramento de dispositivos externos: *Informativo*, *Aviso* e *Crítico*.

      O monitor de integridade do sistema registra informações sobre dispositivos externos conectados no momento em que a linha de base é criada. Subsequentemente, quando um dispositivo externo é conectado, o aplicativo gera um evento correspondente. Ao executar a tarefa, o aplicativo não monitora a desconexão dos dispositivos externos.

6. Salvar alterações.

Configurações de uma regra de tarefa Monitor de integridade do sistema de linha de base

Parâmetro	Descrição
Monitorar operações de arquivos para o escopo	O escopo ao qual se deseja aplicar o Monitor de Integridade de Arquivos. Esse campo é obrigatório. Usar máscaras: O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara: O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas. Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida. O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres \ e / (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres.
Objetos monitorados	Aqui é possível especificar o nome ou o valor de uma chave de registro. Usar máscaras: O Kaspersky Embedded Systems Security é compatível com os caracteres `*` e `?` ao inserir uma máscara:
Exclusões	Na guia **Exclusões**, é possível adicionar os objetos que se deseja excluir do escopo de monitoramento: • Para uma regra do Monitor de Integridade de Arquivos, é possível especificar uma lista de pastas. • Para uma regra do monitor de acesso ao registro, é possível especificar chaves ou valores de registro. Usar máscaras: **Arquivos** Lista de arquivos e pastas monitorados pelo componente. O Kaspersky Embedded Systems Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara: O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas. Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados nas pastas dentro da `Folder` exceto para a `Folder` em si. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida. O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto pelos caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Folder` que tenham a extensão TXT e um nome composto por três caracteres. **Registro** O Kaspersky Embedded Systems Security tem suporte para os caracteres `*` e `?` ao inserir uma máscara: as entradas de exclusão têm uma prioridade mais alta do que as entradas do escopo de monitoramento.
Nível de gravidade do evento	O Kaspersky Embedded Systems Security registra eventos de modificação de arquivo sempre que um arquivo de registro no escopo de monitoramento é modificado. Estão disponíveis os seguintes níveis de gravidade do evento: **Informativo**, **Aviso**, **Crítico**.

Execução da tarefa de Monitor de integridade do sistema de linha de base

A tarefa **Monitor de integridade do sistema de linha de base** permite verificar arquivos ou chaves do registro quanto a alterações e também verificar a conexão de dispositivos externos. Para verificar os arquivos quanto a alterações, é possível executar a tarefa **Monitor de integridade do sistema de linha de base** nos seguintes modos:

- **Verificação completa**. Nesse modo, o aplicativo verifica todos os atributos e hashes de arquivos.
- **Verificação rápida**. Nesse modo, o aplicativo verifica apenas os atributos dos arquivos.

O modo em que a tarefa é executada não afeta a verificação do registro ou dos dispositivos externos.

Como executar a tarefa Monitor de integridade do sistema de linha de base no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Tarefas**.

   A lista de tarefas é aberta.

2. Clique **Nova tarefa**.

   O Assistente de Tarefas é iniciado. Siga as instruções do Assistente.

3. Selecione **Kaspersky Embedded Systems Security → Monitor de integridade do sistema de linha de base**. Selecione um modo do monitor de integridade do sistema:

   - **Verificação completa**. Nesse modo, o aplicativo verifica todos os atributos e hashes de arquivos.
   - **Verificação rápida**. Nesse modo, o aplicativo verifica apenas os atributos dos arquivos.

4. Selecione os computadores nos quais a tarefa será executada. As seguintes opções estão disponíveis:

   - Selecionar computadores detectados pelo Servidor de Administração na rede: dispositivos não atribuídos. Os dispositivos específicos podem incluir dispositivos nos grupos de administração e dispositivos não atribuídos.
   - Especificar endereços de dispositivo manualmente ou importar endereços de uma lista. Você pode especificar nomes de NetBIOS, endereços IP e sub-redes IP de dispositivos aos quais você quer atribuir a tarefa.
   - Especificar a seleção de dispositivos para os quais se deseja executar a tarefa.
   - Atribuir a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos em um grupo de administração criado anteriormente.

5. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Embedded Systems Security inicia a tarefa com os direitos de uma conta de usuário local.

6. Configurar um agendamento para a tarefa, por exemplo, manualmente ou em um determinado dia da semana.

7. Insira o nome da tarefa.

8. Concluir a operação do assistente. Caso seja necessário, marque a caixa de seleção **Executar tarefa após a conclusão do assistente**. Você pode monitorar o andamento da tarefa nas propriedades da tarefa.

Como executar a tarefa Monitor de integridade do sistema de linha de base no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Tarefas**.

   A lista de tarefas é aberta.

2. Clique **Adicionar**.

   O Assistente de Tarefas é iniciado.

3. Defina as configurações da tarefa:

   a. Na lista suspensa **Aplicativo**, selecione Kaspersky Embedded Systems Security.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Monitor de integridade do sistema de linha de base**.

   c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Verificação semanal de integridade do sistema*.

4. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

5. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

6. Selecionar o algoritmo de cálculo da selecionar soma de verificação.

7. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Embedded Systems Security inicia a tarefa com os direitos de uma conta de usuário local.

8. Concluir a operação do assistente.

   Uma nova tarefa será exibida na lista de tarefas.

9. Clique na Nova Tarefa.

   A janela de propriedades da tarefa é exibida.

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

11. Selecione um modo verificação de integridade do sistema:

    - **Verificação completa**. Nesse modo, o aplicativo verifica todos os atributos e hashes de arquivos.
    - **Verificação rápida**. Nesse modo, o aplicativo verifica apenas os atributos dos arquivos.

12. Salvar alterações.

13. Marque a caixa de seleção ao lado da tarefa.

14. Clique **Iniciar**.

Exportação e importação das regras do monitor de integridade do sistema

É possível exportar a lista de regras do monitor de integridade do sistema para um arquivo XML. Em seguida, será possível modificar o arquivo para, por exemplo, adicionar um grande número de regras do mesmo tipo. É possível usar a função de exportar/importar para fazer backup da lista de regras do monitor de integridade do sistema ou para migrar a lista para um servidor diferente.

O Monitor de integridade do sistema não é compatível com a importação de chaves `HKEY_CURRENT_USER` e `HKEY_CURRENT_CONFIG` para a tarefa *Verificação de integridade do sistema*. Caso o escopo de monitoramento da tarefa contenha essas chaves, o aplicativo gerará o evento *O escopo de monitoramento inclui objetos incorretos*.

Como exportar e importar uma lista de regras do monitor de integridade do sistema no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Inspeção do sistema**.
4. Na seção **Monitor de integridade do sistema**, clique no botão **Configurações**.
5. Para exportar o arquivo/regras de registro:
   a. Na guia **Arquivos** ou **Registro**, selecione as regras que deseja exportar.
   b. Clique no botão **Exportar** e selecione **Exportar selecionados**.
   c. Caso não tenha selecionado nenhuma regra, clicar em **Exportar** → **Exportar** fará com que o Kaspersky Embedded Systems Security exporte todas as regras.
   d. Na janela exibida, especifique o nome do arquivo XML para o qual você quer exportar a lista de regras e selecione a pasta na qual você quer salvar esse arquivo.
   e. Salvar o arquivo.
      O Kaspersky Embedded Systems Security exporta toda a lista de regras para o arquivo XML.
6. Para importar o arquivo/regras para registro:
   a. Na guia **Arquivos** ou **Registro**, clique no botão **Importar**.
      Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de regras.

b. Abra o arquivo.

Se o computador já tiver uma lista de regras, o Kaspersky Embedded Systems Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

7. Salvar alterações.

Como exportar e importar uma lista de regras do monitor de integridade do sistema no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Inspeção do sistema** → **Monitor de integridade do sistema** e clique no botão **Configurar**.

   A janela **Configurações do Monitor de integridade do sistema** é aberta.
5. Para exportar o arquivo/regras de registro:

   a. Na guia **Arquivo** ou **Registro**, selecione as regras que deseja exportar.

   b. Clique no botão **Exportar**. Uma janela será aberta; nessa janela, especifique se deseja exportar as regras selecionadas ou todas as regras e, em seguida, clique em **Exportar**.

   Se você não selecionou nenhuma regra, o Kaspersky Embedded Systems Security exportará todas as regras.
6. O Kaspersky Embedded Systems Security exporta toda a lista de regras para o arquivo XML.
7. Para importar o arquivo/regras para registro:

   a. Na guia **Arquivo** ou **Registro**, clique no botão **Importar da versão anterior** caso queira importar as regras de um arquivo XML criado na versão 3.4 ou anterior do aplicativo.

   Caso esteja importando as regras de um arquivo XML criado na versão 4.0 ou posterior, clique em **Importar**.

   b. Se o computador já tiver uma lista de regras, o Kaspersky Embedded Systems Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

   c. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de regras.

   d. Clique **Importar**.
8. Salvar alterações.

Como exportar e importar uma lista de regras do monitor de integridade do sistema no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Inspeção do sistema** → **Monitor de integridade do sistema**.
2. no painel de resultados do node **Monitor de integridade do sistema**, clique no link **Propriedades**.

   A janela **Propriedades: Monitor de integridade do sistema** é aberta.
3. Para exportar o arquivo/regras de registro:

   a. Na guia **Arquivos** ou **Registro**, selecione as regras que deseja exportar.

   b. Clique no botão **Exportar** e selecione **Exportar selecionados**.

   c. Caso não tenha selecionado nenhuma regra, clicar em **Exportar** → **Exportar** fará com que o Kaspersky Embedded Systems Security exporte todas as regras.

   d. Na janela exibida, especifique o nome do arquivo XML para o qual você quer exportar a lista de regras e selecione a pasta na qual você quer salvar esse arquivo.

   e. Salvar o arquivo.

   O Kaspersky Embedded Systems Security exporta toda a lista de regras para o arquivo XML.
4. Para importar o arquivo/regras para registro:

   a. Na guia **Arquivos** ou **Registro**, clique no botão **Importar**.

   Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de regras.

   b. Abra o arquivo.

   Se o computador já tiver uma lista de regras, o Kaspersky Embedded Systems Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.
5. Salvar alterações.

Visualização de relatórios do monitor de integridade do sistema

Para analisar o desempenho das regras do monitor de integridade do sistema, é possível examinar os relatórios e os eventos gerados pelo aplicativo. O Kaspersky Embedded Systems Security gera os seguintes relatórios sobre o componente:

- Na interface do aplicativo:
  - O relatório Atualização da linha de base.

  Os relatórios contém eventos do monitor de integridade do sistema.

- No Console do Kaspersky Security Center
  - Relatório sobre computadores nos quais as regras de monitoramento foram acionadas o maior número de vezes
  - Relatório sobre as regras de monitoramento acionadas com mais frequência

    Para gerar um Relatório sobre as regras de monitoramento acionadas com mais frequência, o aplicativo registra os seguintes eventos:

    - *A alteração de um arquivo ou pasta foi detectada*
    - *Somente para estatística: operação de arquivo proibida em área controlada*
    - *Operação de arquivo permitida em uma área controlada realizada por um usuário confiável*
    - *Operação de arquivo não controlado na área controlada*.

    Para configurar a duração do armazenamento desses eventos, na seção **Configuração de eventos** da política, especifique a duração do evento geral de Monitoramento de Integridade do Sistema: *A alteração de um arquivo ou pasta foi detectada*.

Por padrão, um relatório é criado para os 30 dias anteriores, incluindo a data de criação do relatório.

Como exibir relatórios do monitor de integridade do sistema no Console de Administração do Kaspersky Security Center

1. Abra o Console de Administração do Kaspersky Security Center.
2. No nó **Servidor de Administração** da árvore do Console de Administração, selecione a guia **Relatórios**.
3. Clique **Novo modelo de relatório**.

   O Assistente de novo modelo de relatório é iniciado.
4. Siga as instruções do Assistente de Modelo de Relatório. Na etapa **Selecionar o tipo de modelo de relatório**, selecione o relatório do Monitor de integridade do sistema (a seção **Outro**):
   - **10 dispositivos com acionamento mais frequente das regras do Monitor de integridade de arquivos/Monitor de integridade de arquivos**.
   - **10 regras do Monitor de integridade de arquivos/Monitor de integridade de arquivos acionadas com maior frequência nos dispositivos**.

   Depois que você terminou com o Novo Assistente de Modelo de Relatório, o novo modelo de relatório aparece na tabela na guia **Relatórios**.
5. Abra o relatório clicando duas vezes nele.

O processo de geração do relatório é iniciado. O relatório é exibido em uma nova janela.

Como exibir relatórios do monitor de integridade do sistema no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Monitoramento e relatórios → Relatórios**.
2. Clique **Adicionar**.

   O Assistente de novo modelo de relatório é iniciado.
3. Em **Modelo**, na seção **Outro**, selecione um relatório do monitor de integridade do sistema:

   - **10 dispositivos com acionamento mais frequente das regras do Monitor de integridade de arquivos/Monitor de integridade do sistema**.
   - **10 regras do Monitor de integridade de arquivos/Monitor de integridade do sistema acionadas com maior frequência nos dispositivos**.

   Depois ter concluído o novo assistente de modelo de relatório, o novo modelo de relatório aparecerá na tabela.
4. Selecione e execute o relatório.

O processo de geração do relatório é iniciado. O relatório é exibido em uma nova janela.

Para exibir os eventos gerados pelo aplicativo, também é possível usar as seleções de eventos no console do Kaspersky Security Center.

Inspeção do Log

A inspeção de log monitora a integridade do ambiente protegido de acordo com a análise do log de eventos do Windows. Quando o aplicativo detecta sinais de comportamento atípico no sistema, ele informa ao administrador, pois esse comportamento pode indicar uma tentativa de ataque cibernético.

O Kaspersky Embedded Systems Security analisa os logs de eventos do Windows e detecta violações de acordo com as regras. O componente inclui regras predefinidas. As regras predefinidas são alimentadas por análise heurística. Também é possível adicionar as próprias regras (regras personalizadas). Quando uma regra é acionada, o aplicativo cria um evento com o status *Crítico*.

Caso queira usar a Inspeção de Log, certifique-se de que a política de auditoria esteja configurada e que o sistema esteja registrando os eventos relevantes (para obter detalhes, consulte o site de suporte técnico da Microsoft.).

Parâmetro	Descrição
Regras predefinidas	Lista de regras de Inspeção de Log. As regras predefinidas incluem modelos de atividades anormais no computador protegido. Atividades anormais podem significar uma tentativa de ataque.
Regras personalizadas	Lista de regras de Inspeção de Log adicionadas pelo usuário. É possível definir seus próprios critérios de acionamento da regra de Inspeção de Log. Para fazer isso, é preciso inserir um ID de evento e selecionar uma fonte de evento. É possível selecionar uma fonte de evento entre os logs padrão: *Application*, *Security* ou *System*. Também é possível especificar o log de um aplicativo de terceiros.

Adição de regras personalizadas

É possível definir seus próprios critérios de acionamento da regra de Inspeção de Log. Para fazer isso, é preciso inserir um ID de evento e selecionar uma fonte de evento. É possível procurar o ID de evento no site de suporte técnico da Microsoft. É possível selecionar uma fonte de evento entre os logs padrão: *Application*, *Security* ou *System*. Também é possível especificar o log de um aplicativo de terceiros. É possível descobrir o nome do log do aplicativo de terceiros usando a ferramenta Visualizador de Eventos. Os logs de aplicativos de terceiros são mantidos na pasta Logs de Aplicativos e Serviços (por exemplo, o log *Windows PowerShell*).

O aplicativo não verifica se o log especificado está realmente presente no log de eventos do Windows. Caso haja um erro no nome do log, o aplicativo não monitorará os eventos desse log.

A lista de regras personalizadas já inclui diversas regras criadas pelos especialistas da Kaspersky.

Como adicionar uma regra personalizada no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Inspeção do sistema**.
4. Na seção **Inspeção de log**, clique no botão **Configurações**.

5. Marque a caixa de seleção **Inspeção de log**.
6. No bloco **Regras personalizadas**, marque a caixa de seleção **Aplicar regras personalizadas para Inspeção de log**.
7. Marque as caixas de seleção ao lado das configurações que você deseja editar.
8. Se necessário, clique em **Adicionar** para criar suas próprias regras personalizadas.
9. Uma janela será aberta; nessa janela, configure a regra personalizada:
   - **Nome da regra**.
   - **Nome do log**. Logs de eventos do Windows. Os seguintes logs estão disponíveis: *Application*, *Security*, *System*.
   - **Fonte**. Logs de aplicativos de terceiros. É possível descobrir o nome do log do aplicativo de terceiros usando a ferramenta Visualizador de Eventos. Os logs de aplicativos de terceiros são mantidos na pasta Logs de Aplicativos e Serviços (por exemplo, o log Windows PowerShell).
   - **Identificadores de evento**. IDs de eventos no Log de eventos do Windows. É possível procurar o ID do evento na documentação técnica da Microsoft.
10. Salvar alterações.

Como adicionar uma regra personalizada no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Inspeção do sistema** → **Inspeção de log** e clique no botão **Configurar**.
5. Marque a caixa de seleção **Ativar inspeção de log**.
6. No bloco **Regras personalizadas**, marque a caixa de seleção **Aplicar regras personalizadas para Inspeção do log**.
7. Configurar as regras personalizadas com o uso de botões de alternância:
8. Se necessário, clique em **Adicionar** para criar suas próprias regras personalizadas.
9. Uma janela será aberta; nessa janela, configure a regra personalizada:
   - **Nome da regra**.
   - **Nome do Log de Eventos do Windows**. Logs de eventos do Windows. Os seguintes logs estão disponíveis: *Application*, *Security*, *System*.

- **Fonte**. Logs de aplicativos de terceiros. É possível descobrir o nome do log do aplicativo de terceiros usando a ferramenta Visualizador de Eventos. Os logs de aplicativos de terceiros são mantidos na pasta Logs de Aplicativos e Serviços (por exemplo, o log Windows PowerShell).
- **ID do evento**. IDs de eventos no Log de eventos do Windows. É possível procurar o ID do evento na documentação técnica da Microsoft.

10. Salvar alterações.

Como adicionar uma regra personalizada no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Inspeção do sistema → Inspeção de log**.
2. no painel de resultados do node **Inspeção de log**, clique no link **Propriedades**.

   Esse procedimento abre a janela **Propriedades: Inspeção de log**.
3. Marque a caixa de seleção **Inspeção de log**.
4. No bloco **Regras personalizadas**, marque a caixa de seleção **Aplicar regras personalizadas para Inspeção de log**.
5. Marque as caixas de seleção ao lado das configurações que você deseja editar.
6. Se necessário, clique em **Adicionar** para criar suas próprias regras personalizadas.
7. Uma janela será aberta; nessa janela, configure a regra personalizada:
   - **Nome da regra**.
   - **Nome do log**. Logs de eventos do Windows. Os seguintes logs estão disponíveis: *Application*, *Security*, *System*.
   - **Fonte**. Logs de aplicativos de terceiros. É possível descobrir o nome do log do aplicativo de terceiros usando a ferramenta Visualizador de Eventos. Os logs de aplicativos de terceiros são mantidos na pasta Logs de Aplicativos e Serviços (por exemplo, o log Windows PowerShell).
   - **Identificadores de evento**. IDs de eventos no Log de eventos do Windows. É possível procurar o ID do evento na documentação técnica da Microsoft.
8. Salvar alterações.

Assim, quando a regra for acionada, o Kaspersky Embedded Systems Security criará o evento *Crítico*.

Configuração de regras predefinidas

As regras predefinidas incluem modelos de atividades anormais no computador protegido. Atividades anormais podem significar uma tentativa de ataque. As regras predefinidas são alimentadas por análise heurística. Sete regras predefinidas estão disponíveis para Inspeção de Log. É possível ativar ou desativar essas regras. As regras predefinidas não podem ser excluídas.

É possível configurar os critérios de acionamento de regras que monitoram eventos para as seguintes operações:

- Detecção de força bruta de senha
- Detecção de login de rede

Como configurar as regras predefinidas no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Inspeção do sistema**.
4. Na seção **Inspeção de log**, clique no botão **Configurações**.
5. Marque a caixa de seleção **Inspeção de log**.
6. No bloco **Regras predefinidas**, marque a caixa de seleção **Aplicar regras predefinidas para Inspeção de log**.
7. Marque ou desmarque as caixas de seleção para configurar as regras predefinidas:
   - **Há padrões de um possível ataque de força bruta no sistema**.
   - **Há uma atividade atípica detectada durante a sessão de logon na rede**.
   - **Há padrões de uma possível violação do Log de Eventos do Windows**.
   - **Ações atípicas detectadas em nome de um novo serviço instalado**.
   - **Detectado logon atípico que usa credenciais explícitas**.
   - **Existem padrões de um possível ataque PAC se passando por Kerberos (MS14-068) no sistema**.
   - **Alterações suspeitas detectadas no grupo de administradores integrado privilegiado**.
8. Caso seja necessário, configure a regra **Há padrões de um possível ataque de força bruta no sistema**:
   a. Clique no botão **Configurações** abaixo da regra.
   b. Na janela aberta, especifique o número de tentativas e um período dentro do qual as tentativas de inserir uma senha devem ser executadas para que a regra seja acionada.
   c. Clique em **OK**.
9. Se tiver selecionado a regra **Há uma atividade atípica detectada durante a sessão de logon na rede**, será preciso definir suas configurações:
   a. Clique no botão **Configurações** abaixo da regra.
   b. Na janela que é aberta, no bloco **Detecção de logon na rede**, especifique o início e o fim do intervalo de tempo.

O Kaspersky Embedded Systems Security considera as tentativas de logon realizadas durante o intervalo definido como atividade anormal.

Como padrão, o intervalo não é definido e o aplicativo não monitora tentativas de logon. Para que o aplicativo monitore continuamente as tentativas de logon, defina o intervalo entre 0h e 23h59. O início e o término fdo intervalo não deverão coincidir. Se forem os mesmos, o aplicativo não vai monitorar as tentativas de logon.

c. Crie a lista de usuários confiáveis e endereços IP confiáveis (IPv4 e IPv6).

É possível selecionar usuários no Active Directory, na lista de contas no Kaspersky Security Center ou ao inserir um nome de usuário local manualmente. A Kaspersky recomenda usar contas de usuário locais somente em casos especiais quando não for possível usar contas de usuário de domínio. O Kaspersky Embedded Systems Security não monitora as tentativas de logon desses usuários e computadores.

A exclusão de computadores confiáveis por endereço IP não funciona no aplicativo executado no Windows XP.

d. Clique **OK**.

10. Salvar alterações.

Como configurar as regras predefinidas no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Inspeção do sistema** → **Inspeção de log** e clique no botão **Configurar**.
5. Marque a caixa de seleção **Ativar inspeção de log**.
6. No bloco **Regras predefinidas**, marque a caixa de seleção **Aplicar regras predefinidas para Inspeção de log**.
7. Configurar as regras predefinidas com o uso de botões de alternância:

   - **Há padrões de um possível ataque de força bruta no sistema**.
   - **Há uma atividade atípica detectada durante a sessão de logon na rede**.
   - **Há padrões de uma possível violação do Log de Eventos do Windows**.
   - **Ações atípicas detectadas em nome de um novo serviço instalado**.
   - **Detectado logon atípico que usa credenciais explícitas**.
   - **Existem padrões de um possível ataque PAC se passando por Kerberos (MS14-068) no sistema**.
   - **Alterações suspeitas detectadas no grupo de administradores integrado privilegiado**.

8. Na guia **Estendido** defina as seguintes configurações:

   - Número de tentativas e um período dentro do qual as tentativas de inserir uma senha devem ser executadas para que a regra **Há padrões de um possível ataque de força bruta no sistema** seja acionada.

   - Para a regra **Há uma atividade atípica detectada durante a sessão de logon na rede** ser acionada, especifique o início e o fim do intervalo de tempo durante os quais o aplicativo considerará todas as tentativas de logon como atividade anormal.

     Como padrão, o intervalo não é definido e o aplicativo não monitora tentativas de logon. Para que o aplicativo monitore continuamente as tentativas de logon, defina o intervalo entre 0h e 23h59. O início e o término fdo intervalo não deverão coincidir. Se forem os mesmos, o aplicativo não vai monitorar as tentativas de logon.

9. Criar a lista de usuários confiáveis e endereços IP confiáveis (IPv4 e Ipv6) nas guias correspondentes.

   É possível selecionar os usuários na lista de contas ou inserir manualmente um nome de usuário local.

   > A exclusão de computadores confiáveis por endereço IP não funciona no aplicativo executado no Windows XP.

10. Salvar alterações.

Como configurar regras predefinidas no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Inspeção do sistema → Inspeção de log**.

2. no painel de resultados do node **Inspeção de log**, clique no link **Propriedades**.

   Esse procedimento abre a janela **Propriedades: Inspeção de log**.

3. Marque a caixa de seleção **Inspeção de log**.

4. No bloco **Regras predefinidas**, marque a caixa de seleção **Aplicar regras predefinidas para Inspeção de log**.

5. Marque ou desmarque as caixas de seleção para configurar as regras predefinidas:

   - **Há padrões de um possível ataque de força bruta no sistema**.
   - **Há uma atividade atípica detectada durante a sessão de logon na rede**.
   - **Há padrões de uma possível violação do Log de Eventos do Windows**.
   - **Ações atípicas detectadas em nome de um novo serviço instalado**.
   - **Detectado logon atípico que usa credenciais explícitas**.
   - **Existem padrões de um possível ataque PAC se passando por Kerberos (MS14-068) no sistema**.
   - **Alterações suspeitas detectadas no grupo de administradores integrado privilegiado**.

6. Caso seja necessário, configure a regra **Há padrões de um possível ataque de força bruta no sistema**:

   a. Clique no botão **Configurações** abaixo da regra.

   b. Na janela aberta, especifique o número de tentativas e um período dentro do qual as tentativas de inserir uma senha devem ser executadas para que a regra seja acionada.

   c. Clique em **OK**.

7. Se tiver selecionado a regra **Há uma atividade atípica detectada durante a sessão de logon na rede**, será preciso definir suas configurações:

   a. Clique no botão **Configurações** abaixo da regra.

   b. Na janela que é aberta, no bloco **Detecção de logon na rede**, especifique o início e o fim do intervalo de tempo.

   O Kaspersky Embedded Systems Security considera as tentativas de logon realizadas durante o intervalo definido como atividade anormal.

   Como padrão, o intervalo não é definido e o aplicativo não monitora tentativas de logon. Para que o aplicativo monitore continuamente as tentativas de logon, defina o intervalo entre 0h e 23h59. O início e o término fdo intervalo não deverão coincidir. Se forem os mesmos, o aplicativo não vai monitorar as tentativas de logon.

   c. Crie a lista de usuários confiáveis e endereços IP confiáveis (IPv4 e IPv6).

   É possível selecionar usuários no Active Directory, na lista de contas no Kaspersky Security Center ou ao inserir um nome de usuário local manualmente. A Kaspersky recomenda usar contas de usuário locais somente em casos especiais quando não for possível usar contas de usuário de domínio. Criar a lista de usuários pelo Active Directory. O Kaspersky Embedded Systems Security não monitora as tentativas de logon desses usuários e computadores.

   > A exclusão de computadores confiáveis por endereço IP não funciona no aplicativo executado no Windows XP.

   d. Clique **OK**.

8. Salvar alterações.

Assim, quando a regra é acionada, o Kaspersky Embedded Systems Security cria o evento *Crítico*.

Verificação sob 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 verifica a área especificada quanto à existência de vírus e outras ameaças à segurança do computador. O Kaspersky Embedded Systems Security verifica arquivos, RAM e objetos de execução automática do dispositivo protegido.

O Kaspersky Embedded Systems Security oferece as seguintes tarefas de Verificação por demanda:

- Por padrão, a tarefa de *Verificação de áreas críticas* é executada semanalmente conforme agendamento. O Kaspersky Embedded Systems Security 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 Kaspersky Embedded Systems Security aplica as configurações de segurança correspondentes ao nível **Informar**. É possível modificar as configurações da tarefa de *Verificação de áreas críticas*.

- A tarefa Verificação de integridade do aplicativo é executada diariamente. Ela fornece a opção de verificar módulos do Kaspersky Embedded Systems Security 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.

- A tarefa *Verificação de unidades removíveis* verifica todos os arquivos executados ou copiados, mesmo que o arquivo esteja localizado em uma unidade removível. Para evitar a propagação de vírus e outros malwares, é possível configurar as verificações automáticas de unidades removíveis quando elas estiverem conectadas ao computador.

- A tarefa *Verificação completa* é executada semanalmente. A tarefa garante uma verificação completa do dispositivo protegido, inclusive do armazenamento de backup do sistema, setores de inicialização e bancos de dados de e-mail.

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 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 com uma lista dos recursos de arquivo do dispositivo protegido que o Kaspersky Embedded Systems Security pode controlar.

Os itens ou nós são exibidos em um modo de visualização de lista dos recursos de arquivo do dispositivo protegido, como se segue:

☑ O nó está incluído no escopo de verificação.

☐ O nó é excluído do escopo de verificação.

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 lista de recursos de arquivos do dispositivo.

Caso o mesmo objeto esteja incluído em várias entradas do escopo de proteção e essas entradas tiverem níveis de segurança diferentes, a última regra na lista terá prioridade. Por exemplo, considere um escopo de proteção que inclua duas entradas: **Todos os discos rígidos** (nível de segurança **Informar**) e `*\Users\*\Downloads\*` (nível de segurança **Personalizado**). O aplicativo verifica os discos rígidos de acordo com o nível Informar, exceto a pasta `Downloads`. O aplicativo verifica a pasta `Downloads` de acordo com as configurações especificadas manualmente porque essa entrada é a última na lista do escopo de proteção.

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 nós ou itens selecionados na lista dos recursos de arquivo do dispositivo protegido (o nível de segurança é alterado para **Personalizado**).

Escopos de verificação predefinidos

A lista de recursos de arquivo do dispositivo protegido para a tarefa de Verificação por demanda selecionada é exibida na janela **Escopo da verificação**.

A 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 contém os escopos de verificação predefinidos a seguir:

- **Todos os discos rígidos**. O Kaspersky Embedded Systems Security 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.
- **Todas as unidades removíveis**. O Kaspersky Embedded Systems Security 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.
- **Todas as unidades de 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 Kernel**. O Kaspersky Embedded Systems Security verifica os arquivos executáveis e módulos dos processos em execução no sistema operacional quando a verificação é iniciada.
- **Executando processos e Objetos de inicialização**. O Kaspersky Embedded Systems Security 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.
- **Setores de inicialização do disco**. O Kaspersky Embedded Systems Security verifica os setores de inicialização de discos rígidos e mídias removíveis.
- **Meu e-mail**. O Kaspersky Embedded Systems Security verifica os arquivos relevantes para o cliente de e-mail do Outlook: arquivos de dados (PST), arquivos de dados offline (OST).
- **Backup do sistema**. O Kaspersky Embedded Systems Security verifica os conteúdos da pasta Informações sobre o volume do sistema.

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 de áreas críticas*:
  - **Todos os discos rígidos** (exceto as pastas do Windows).
  - **Todas as unidades removíveis**.
  - **Memória Kernel**.
  - **Executando processos e Objetos de inicialização**.

- Tarefa de *Verificação por demanda*:
  - **Todos os discos rígidos** (exceto as pastas do Windows).
  - **Todas as unidades removíveis**.
  - **Memória Kernel**.
  - **Executando processos e Objetos de inicialização**.
- Tarefa de *Verificação completa*:
  - **Todos os discos rígidos** (exceto as pastas do Windows).
  - **Todas as unidades removíveis**.
  - **Memória Kernel**.
  - **Executando processos e Objetos de inicialização**.
  - **Backup do sistema**.
  - **Setores de inicialização do disco**.
  - **Meu e-mail**.

Verificação de arquivos no armazenamento on-line

Sobre arquivos na nuvem

O Kaspersky Embedded Systems Security 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 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 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 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 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 proibição para arquivos e com o uso da 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

> A configuração de segurança **Usar a análise heurística** não está incluída nas configurações para os níveis de segurança predefinidos. A alteração dessa configuração não mudará o nível de segurança padrão selecionado.

É possível aplicar um dos quatro níveis de segurança predefinidos a um nó selecionado na árvore de recursos de arquivos do dispositivo: **Desempenho máximo**, **Recomendado**, **Proteção máxima** ou **Informar**. 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 caso a rede tenha medidas de segurança adicionais nos dispositivos protegidos, como firewalls e políticas de segurança existentes, além de usar o Kaspersky Embedded Systems Security nos dispositivos e estações de trabalho 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.

Informar

O nível de segurança **Informar** é recomendado caso haja muitos computadores com potencial de infecção na rede corporativa e o bloqueio desses computadores possa interromper significativamente a operação da organização.

Níveis de segurança predefinidos e valores de configurações de segurança correspondentes

Opções	Nível de segurança			
Desempenho máximo	Recomendado	Proteção máxima	Informar	
Tipos de objetos	Objetos verificados por formato	Todos os objetos	Todos os objetos	Todos os objetos
Verificar somente arquivos novos e alterados	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	Informações
Verificação de arquivos compostos	Verificar os pacotes de distribuição e arquivos nos formatos do Microsoft Office	Verificar todos os arquivos compactados, pacotes de distribuição e arquivos nos formatos do Microsoft Office	Verificar todos os arquivos compactados, pacotes de distribuição e arquivos nos formatos do Microsoft Office	Verificar todos os arquivos compactados, pacotes de distribuição e arquivos nos formatos do Microsoft Office
Os objetos críticos do sistema são arquivos necessários para a operação do sistema operacional e do Kaspersky Embedded Systems Security. Esses arquivos não podem ser excluídos. Os processos associados a esses objetos não podem ser encerrados.				
Aplicar a ação aos tipos de objetos selecionados	Por padrão, todos os tipos de objetos são verificados	Por padrão, todos os tipos de objetos são verificados	Por padrão, todos os tipos de objetos são verificados	Por padrão, todos os tipos de objetos são verificados
Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado	Não	Não	Não	Não

Opções	Nível de segurança			
Excluir arquivos	Não	Não	Não	Não
Não detectar objetos por tipo	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
Usar tecnologia iSwift	Sim	Sim	Sim	Sim
Usar tecnologia iChecker	Sim	Sim	Sim	Sim

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 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 Kaspersky Embedded Systems Security 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

Parâmetro	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 unidade removível se o tamanho não exceder (MB)	4096 MB	É possível reduzir o escopo do componente configurando o volume máximo de dados na unidade verificada. O Kaspersky Embedded Systems Security 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** • **Informar**. 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.

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

Parâmetro	Valor padrão	Descrição
Escopo da verificação	Aplicado em tarefas locais do sistema e tarefas personalizadas: • **Verificação de áreas críticas**: o dispositivo protegido inteiro, excluindo pastas compartilhadas e certos arquivos de sistema operacional. • **Verificação por demanda** (tarefas personalizadas): o dispositivo protegido inteiro. • **Verificação completa**: uma verificação detalhada do dispositivo protegido.	Você pode alterar o escopo da verificação. O escopo da verificação não pode ser configurado para as tarefas locais do sistema **Verificação de unidades removíveis** e **Controle de Integridade de Aplicativos**.
Configurações de segurança	As configurações comuns de todo o escopo da verificação correspondem ao nível de segurança **Recomendado**.	Para os nós selecionados na lista de recursos de arquivo do dispositivo protegido, é possível: • Selecionar um nível de segurança predefinido diferente • Alterar manualmente as configurações de segurança
Usar a análise heurística	Aplicado com o nível de análise **Médio** para as tarefas *Verificação de áreas críticas*, *Verificação por demanda* e *Verificação completa*.	É possível ativar ou desativar o Analisador Heurístico e configurar o nível de análise.
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 a tarefa *Verificação de integridade do aplicativo*.
Executar tarefa em segundo plano	Não aplicado	Você pode configurar o nível de prioridade das tarefas de Verificação por Demanda.
Considerar tarefa como Verificação de áreas críticas	Aplicada para as tarefas *Verificação por demanda*, *Verificação de áreas críticas* e *Verificação completa*.	Você pode configurar o nível de prioridade das tarefas de Verificação por Demanda.
Não executar várias tarefas de verificação ao mesmo tempo	Não aplicado	Você pode configurar o nível de prioridade das tarefas de Verificação por Demanda.
Programação de inicialização da tarefa	Aplicada em tarefas locais do sistema: *Verificação de áreas críticas*, *Verificação de integridade do aplicativo* e *Verificação completa* – **Mensalmente**.	É possível definir as configurações para o início de uma tarefa programada.

Sobre tarefas de Verificação por Demanda

Esta seção descreve a navegação na interface e as definições das configurações da tarefa Verificação por demanda no dispositivo protegido.

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 criar uma nova tarefa de Verificação por demanda:

[Vá para o assistente de nova tarefa para criar uma tarefa de Verificação por demanda no Console de Administração do Kaspersky Security Center]

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 nó **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. Selecione a guia **Tarefas**.
   d. Clique **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. Selecione a guia **Selecionar resultados "nome da seleção"**.
   c. Na lista suspensa **Executar ação**, selecione **Nova tarefa**.

   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.

5. Clique em **Avançar** e configure a tarefa conforme seja 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.

[Vá para o assistente de nova tarefa para criar uma tarefa de verificação por demanda no Kaspersky Security Center Web Console]

1. Na janela principal do Web Console, selecionar **Dispositivos** → **Dispositivos gerenciados**.

2. Clique no nome do dispositivo protegido.

3. Na janela **<Nome do dispositivo>** que é exibida, selecione a guia **Tarefas**.

4. Clique no botão **Adicionar**.
   A janela **Assistente de Nova Tarefa** será aberta.

5. Na lista suspensa **Aplicativo**, selecione **Kaspersky Embedded Systems Security**.

6. Na lista suspensa **Tipo de tarefa**, selecione a tarefa de **Verificação por demanda**.

7. Clique em **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, selecionar **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**.

5. Na lista suspensa **Tipo de tarefa**, selecione a tarefa de **Verificação por demanda**.

6. Clique em **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.Clique no botão Nova tarefa.Clique no botão **Nova tarefa**.
6. Na lista suspensa **Aplicativo**, selecione **Kaspersky Embedded Systems Security**.
7. Na lista suspensa **Tipo de tarefa**, selecione a tarefa de **Verificação por demanda**.
8. Clique em **Avançar**.

   Defina as configurações da tarefa conforme necessário.

Para configurar uma tarefa de Verificação por Demanda existente:

1. Na janela principal do Web Console, selecionar **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 configurações da tarefa de Verificação por Demanda

Para abrir as configurações do aplicativo para a tarefa de Verificação por Demanda para um único dispositivo protegido:

Para abrir as configurações gerais da tarefa Verificação por Demanda no Console de Administração do Kaspersky Security Center

1. Expanda o nó **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.

Para abrir as configurações gerais da tarefa Verificação por Demanda no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecionar **Dispositivos** → **Dispositivos gerenciados**.
2. Selecione 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**.

Para abrir as configurações gerais da tarefa de Verificação por demanda no Console do Aplicativo

1. Na árvore do Console do Aplicativo, expanda o nó **Verificação por demanda**.
2. Selecione o nó secundário que corresponde à tarefa que deseja configurar.
3. No painel de resultados do nó secundário, clique no link **Propriedades**.

   A janela **Propriedades: <Nome da tarefa>** é exibida.

Criando uma tarefa de Verificação por Demanda

Criando uma tarefa de Verificação por demanda no Console de Administração do Kaspersky Security Center

1. Inicie o assistente de nova tarefa.
2. Na janela **Selecionar tipo de tarefa**, selecione **Verificação por demanda** e clique em **Avançar**.
3. 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 algum escopo da verificação, selecione o item da lista correspondente e clique em **Excluir**.
- Para incluir um escopo de verificação predefinido, um disco, uma pasta, um objeto de rede ou um arquivo no escopo da verificação:
  a. Clique **Adicionar**.
  b. Na janela **Selecionar escopo da verificação**, selecione o escopo da verificação predefinido da lista e clique em **OK**.
- Para excluir subpastas ou arquivos do escopo da verificação:
  a. Selecione uma pasta adicionada (ou disco) na janela **Escopo da verificação**.
  b. Clique **Editar**.
  c. Desmarcar a caixa de seleção **Incluir subpastas**
- Para alterar as configurações de segurança do escopo da verificação:
  a. Selecione o escopo da verificação para o qual deseja editar as configurações e clique em **Configurar**.
  b. Esse procedimento abre uma janela; nessa janela, selecione um dos níveis de segurança predefinidos ou clique no botão **Configurações** para definir manualmente as configurações de segurança.

As configurações de segurança são definidas do mesmo modo para a tarefa Proteção de Arquivos em Tempo Real.

4. Configurar o Analisador Heurístico e a integração com outros componentes:
   - Configurar o uso do analisador heurístico.
   - Marque a caixa de seleção **Executar tarefa em segundo plano** caso queira atribuir a prioridade *Baixa* ao processo de trabalho no qual a tarefa será executada.

     Por padrão, os processos de trabalho em que as tarefas do Kaspersky Embedded Systems Security são executadas têm prioridade *Média* (Normal).
   - Marque a caixa de seleção **Considerar tarefa como Verificação de áreas críticas** caso queira usar a tarefa como uma tarefa de *Verificação de áreas críticas*.
   - Marque a caixa de seleção **Não executar várias tarefas de verificação ao mesmo tempo** para otimizar a carga do computador.

5. Na janela **Selecionar os dispositivos aos quais a tarefa será atribuída**, especifique a lista de dispositivos e clique em **Avançar**.

6. Na janela **Selecionar uma conta para executar a tarefa**, especifique uma conta e clique em **Avançar**.

7. Na janela **Configurar agendamento da tarefa**, configure o agendamento da tarefa e clique em **Avançar**.

8. Insira o nome da tarefa.

   O nome da tarefa não deve ter mais de 100 caracteres e não pode conter os seguintes símbolos: " * < > & \ : |

9. A janela **Concluir a criação da tarefa** é aberta. 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.

Criando uma tarefa de Verificação por demanda no Kaspersky Security Center Web Console

1. Inicie o assistente de nova tarefa.

2. Na janela **Nova tarefa**, na lista suspensa **Aplicativo**, selecione **Kaspersky Embedded Systems Security**.

3. Na lista suspensa **Tipo de tarefa**, selecione **Verificação por demanda** e clique em **Avançar**.

4. Selecione o escopo da tarefa e clique em **Avançar**.

5. Na janela **Selecionar uma conta para executar a tarefa**, especifique uma conta e clique em **Avançar**.

6. Insira o nome da tarefa.

   O nome da tarefa não deve ter mais de 100 caracteres e não pode conter os seguintes símbolos: " * < > & \ : |

7. A janela **Concluir a criação da tarefa** é aberta. 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.

Criando uma tarefa de Verificação por demanda no Console do Aplicativo

É possível criar tarefas personalizadas para um único dispositivo protegido no node **Verificação por demanda**.

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 a opção **Criar tarefa**.

   A janela **Criar tarefa** é aberta.
3. Insira um nome para a tarefa e clique em **OK**.

A tarefa Verificação por demanda para um dispositivo protegido individual é criada.

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 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.

Para alterar a prioridade de uma tarefa de Verificação por demanda existente, marque ou desmarque a caixa de seleção **Executar tarefa em segundo plano** nas configurações da tarefa.

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 nó do **Kaspersky Embedded Systems Security** e atualizado semanalmente após a execução da tarefa de *Verificação de áreas críticas*.

A hora que o status de proteção do dispositivo é atualizado será vinculada ao agendamento da tarefa de Verificação por demanda para a qual a caixa de seleção **Considerar tarefa como Verificação de áreas críticas** estiver marcada.

Configurando o escopo da verificação na tarefa Verificação por Demanda

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 ao reparar o próprio Kaspersky Embedded Systems Security com o uso do Assistente de instalação.

Configurando o escopo da verificação para a tarefa Verificação por demanda no Console de Administração do Kaspersky Security Center

1. Abra a janela **Propriedades: Verificação por demanda**.
2. Selecione a seção **Escopo da verificação**.
3. Para adicionar escopos ao escopo da verificação, marque as caixas de seleção ao lado deles.
4. Caso queira adicionar um escopo de verificação que não esteja na lista:
   a. Clique **Adicionar**.
   b. Na janela exibida, selecione um escopo, um disco individual, uma pasta ou um local de rede.
   c. Caso queira incluir subpastas no escopo da verificação, marque a caixa de seleção **Incluir subpastas**.
5. Para excluir nós individuais do escopo da verificação, desmarque as caixas ao lado dos nomes destes nós.
6. Para editar um escopo da verificação, selecione o escopo da verificação na lista e clique em **Editar**.
7. Para esconder um escopo da verificação anteriormente adicionado da lista de recursos de arquivos de rede, selecione o escopo da verificação e clique em **Excluir**.

   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.

8. Clique em **OK**.

A janela Configurações do escopo da verificação é fechada. As configurações recém-definidas são salvas.

Configurando o escopo da verificação para a tarefa Verificação por demanda no Kaspersky Security Center Web Console

1. Abra a janela **Verificação por demanda**.
2. Selecione a guia **Configurações do aplicativo**.
3. Para adicionar escopos ao escopo da verificação, marque as caixas de seleção ao lado deles e defina o botão de alternância para Ligado.
4. Caso queira adicionar um escopo de verificação que não esteja na lista:
   a. Clique **Adicionar**.
   b. Na janela exibida, selecione um escopo, um disco individual, uma pasta ou um local de rede.
   c. Caso queira incluir subpastas no escopo da verificação, marque a caixa de seleção **Subpastas**.
5. Para excluir nós individuais do escopo da verificação, desmarque as caixas ao lado dos nomes destes nós.

6. Para editar um escopo da verificação, selecione o escopo da verificação na lista e clique em **Editar escopo**.

7. Para esconder um escopo da verificação anteriormente adicionado da lista de recursos de arquivos de rede, selecione o escopo da verificação e clique em **Excluir**.

   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.

8. Clique **Salvar**.

A janela Configurações do escopo da verificação é fechada. As configurações recém-definidas são salvas.

Configurando o escopo da verificação da tarefa de Verificação por demanda no Console do Aplicativo

1. Na árvore do Console do Aplicativo, expanda o nó **Verificação por demanda**.

2. Selecione o nó 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 de proteção**.

4. Na janela exibida, para adicionar escopos ao escopo da verificação, marque as caixas de seleção ao lado deles.

5. Caso queira adicionar um escopo de verificação que não esteja na lista:

   a. Clique **Adicionar**.

   b. Na janela exibida, selecione um escopo, um disco individual, uma pasta ou um local de rede.

   c. Caso queira incluir subpastas no escopo da verificação, marque a caixa de seleção **Incluir subpastas**.

6. Para excluir nós individuais do escopo da verificação, desmarque as caixas ao lado dos nomes destes nós.

7. Para editar um escopo da verificação, selecione o escopo da verificação na lista e clique em **Editar escopo**.

8. Para esconder um escopo da verificação anteriormente adicionado da lista de recursos de arquivos de rede, selecione o escopo da verificação e clique em **Excluir**.

   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.

9. Clique **OK**.

A janela Configurações do escopo da verificação é fechada. As configurações recém-definidas são salvas.

Abertura das configurações da tarefa de Verificação por Demanda

Como configurar a tarefa Verificação por demanda no Console de Administração do Kaspersky Security Center

1. Abra as propriedades da tarefa de Verificação por Demanda.
2. Selecione a seção **Opções**.
3. Desmarque ou marque a caixa de seleção **Usar a análise heurística**.
4. Caso seja necessário, altere o nível da análise.
5. Marque a caixa de seleção **Executar tarefa em segundo plano** caso queira atribuir a prioridade *Baixa* ao processo de trabalho no qual a tarefa será executada.

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

6. Marque a caixa de seleção **Considerar tarefa como Verificação de áreas críticas** caso queira usar a tarefa como uma tarefa de *Verificação de áreas críticas*.
7. Marque a caixa de seleção **Não executar várias tarefas de verificação ao mesmo tempo** para otimizar a carga do computador.
8. Salvar alterações.

Como configurar a tarefa Verificação por demanda no Kaspersky Security Center Web Console

1. Abra as propriedades da tarefa de Verificação por Demanda.
2. Selecione a seção **Configurações do aplicativo**.
3. Ir para a seção **Configurações**.
4. Desmarque ou marque a caixa de seleção **Usar a análise heurística**.
5. Caso seja necessário, selecione o nível de análise na lista suspensa **Nível de análise heurística**.

6. Marque a caixa de seleção **Executar tarefa em segundo plano** caso queira atribuir a prioridade *Baixa* ao processo de trabalho no qual a tarefa será executada.

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

7. Marque a caixa de seleção **Considerar tarefa como Verificação de áreas críticas** caso queira usar a tarefa como uma tarefa de *Verificação de áreas críticas*.

8. Marque a caixa de seleção **Não executar várias tarefas de verificação ao mesmo tempo** para otimizar a carga do computador.

9. Salvar alterações.

Como configurar a tarefa de Verificação por demanda no Console do Aplicativo

1. Na árvore do Console do Aplicativo, expanda o nó **Verificação por demanda**.

2. Selecione o nó secundário que corresponde a uma tarefa de Verificação por Demanda que deseja configurar.

3. No painel de resultados do node selecionado, clique no link **Propriedades**.

4. Selecione a guia **Configurações da tarefa**.

5. Desmarque ou marque a caixa de seleção **Usar a análise heurística**.

6. Caso seja necessário, altere o nível da análise.

7. Marque a caixa de seleção **Executar tarefa em segundo plano** caso queira atribuir a prioridade *Baixa* ao processo de trabalho no qual a tarefa será executada.

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

8. Marque a caixa de seleção **Considerar tarefa como Verificação de áreas críticas** caso queira usar a tarefa como uma tarefa de *Verificação de áreas críticas*.

9. Marque a caixa de seleção **Não executar várias tarefas de verificação ao mesmo tempo** para otimizar a carga do computador.

10. Salvar alterações.

Configuração da Verificação de Unidades Removíveis

Configurando a Verificação de unidades removíveis no Kaspersky Security Center Administration Console

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 configurar a tarefa.
3. Selecione a etiqueta **de políticas**.
4. Clique duas vezes no nome da política que você quer configurar.

   Na janela de propriedades da política, acesse a seção **Suplementar**.
5. Clique em **Configurações** na subseção **Verificação de unidades removíveis**.

   A janela **Verificação de unidades removíveis** é aberta.
6. Faça o seguinte:

   - Marque a caixa de seleção **Verificar unidades removíveis ao conectar via USB**, se desejar que o Kaspersky Embedded Systems Security verifique automaticamente as unidades removíveis quando elas forem conectadas.
   - Se necessário, selecione **Verificar unidade removível se o tamanho 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 em **OK**.

As configurações específicas são salvas e aplicadas.

Configurando a Verificação de unidades removíveis no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Ir para a seção **Suplementar**.
5. Clique em **Configurar** em **Verificação de unidades removíveis**.

   A janela **Verificação de unidades removíveis** é aberta.

6. Faça o seguinte:

   - Marque a caixa de seleção **Verificar unidades removíveis ao conectar via USB**, se desejar que o Kaspersky Embedded Systems Security verifique automaticamente as unidades removíveis quando elas forem conectadas.
   - Se necessário, selecione **Verificar unidade removível se o tamanho 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 em **OK**.

As configurações específicas são salvas e aplicadas.

Configurando a Verificação de unidades removíveis no Console do Aplicativo

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security** e selecione **Verificação de unidades removíveis**.

   A janela **Verificação de unidades removíveis** é aberta.

2. Faça o seguinte:

   - Marque a caixa de seleção **Verificar unidades removíveis ao conectar via USB**, se desejar que o Kaspersky Embedded Systems Security verifique automaticamente as unidades removíveis quando elas forem conectadas.
   - Se necessário, selecione **Verificar unidade removível se o tamanho 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 **OK**.

Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda

É possível aplicar um dos seguintes três níveis de segurança predefinidos em um nó selecionado na lista de recursos de arquivos do dispositivo protegido: **Desempenho máximo**, **Recomendado** e **Proteção máxima**.

Selecione um dos níveis de segurança predefinidos na seção do Console de Administração do Kaspersky Security Center

1. Abra as propriedades da tarefa de Verificação por Demanda.
2. Selecione a seção **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 **Configurar**.
5. Esse procedimento abre uma janela; nessa janela, na guia **Nível de segurança**, selecione o nível de segurança que será aplicado.
6. Clique **OK**.
7. Na janela **Propriedades: Verificação por demanda**, 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.

Selecione um dos níveis de segurança predefinidos no Console do Aplicativo

1. Na árvore do Console do Aplicativo, expanda o nó **Verificação por demanda**.
2. Selecione o nó 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 de proteção**.
4. Na lista de recursos de arquivos de rede do dispositivo protegido, selecione um nó ou item para o qual se deseja definir o nível de segurança predefinido.
5. Certifique-se de que o node ou item selecionado seja incluído no escopo da verificação.
6. Clique **Configurar**.
7. Esse procedimento abre uma janela; nessa janela, selecione o nível de segurança de sua escolha.

   A janela exibe a lista de configurações de segurança correspondentes ao nível de segurança selecionado.
8. Clique **OK**.

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.

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.

Gerenciando manualmente as configurações de segurança no Console de Administração do Kaspersky Security Center

1. Abra as propriedades da tarefa de Verificação por Demanda.
2. Selecione a seção **Escopo da verificação**.
3. Na lista de dispositivos protegidos, selecione um item incluído no escopo da verificação para gerenciar as configurações de segurança.
4. Clique **Configurar**.
5. Esse procedimento abre uma janela; nessa janela, na guia **Nível de segurança**, selecione o nível de segurança que será aplicado.
6. Selecione o recurso para o qual deseja definir as configurações de segurança.
7. Clique **Configurar**.
8. Na janela que é aberta, selecione o nível de segurança necessário e clique em **Configurações**..
9. Na guia **Geral**, defina as seguintes configurações:
   - Objetos que devem ser incluídos no escopo de proteção:
     - **Todos os objetos**
     - **Objetos verificados por formato**
     - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**
   - Na seção **Otimização**, marque ou desmarque a caixa de seleção **Proteger somente arquivos novos e modificados**.
   - Na seção **Verificação de arquivos compostos**, especifique os objetos compostos que deseja incluir no escopo da verificação:
     - **Verificar arquivos comprimidos**

- Verificar pacotes de distribuição
- Verificar arquivos de formatos do Microsoft Office
- Verificar arquivos de formato de e-mail

10. Na guia **Ações**, defina as seguintes configurações:

- Selecione a ação a ser executada em objetos infectados e outros objetos detectados:
  - **Desinfectar**
  - **Desinfectar e excluir se a desinfecção falhar**
  - Excluir
  - Recomendado
  - Informar
- Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:
  a. Desmarque ou marque a caixa de seleção Aplicar a ação aos tipos de objetos selecionados.
  b. Clique em **Configurações** e selecione os tipos de objetos que serão detectados.
- Configurar as ações em arquivos compostos que não estejam disponíveis para modificação: desmarque ou marque a caixa de seleção Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado.

11. Na guia **Desempenho**, defina as seguintes configurações:

- No bloco **Exclusões**:
  - Desmarque ou marque a caixa de seleção Excluir arquivos.
  - Desmarque ou marque a caixa de seleção Não detectar objetos por tipos.
    Clique no botão **Editar** de cada configuração para adicionar exclusões.
- 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

12. Salvar as novas configurações de segurança.

1. Abra as propriedades da tarefa de Verificação por Demanda.
2. Selecione a seção **Configurações do aplicativo**.
3. Ir para a seção **Escopo da verificação**.
4. Na lista de recursos de arquivos de rede do dispositivo protegido, selecione um item para o qual deseja gerenciar as configurações de segurança. Certifique-se de que o node ou item selecionado seja incluído no escopo da verificação.
5. Clique **Editar**.
6. Selecione um modo de proteção de objetos na lista suspensa:
   - **Todos os objetos**
   - **Objetos verificados por formato**
   - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**
7. Marque ou desmarque a caixa de seleção **Proteger somente arquivos novos e modificados** e especifique se deseja incluir Subpastas na verificação.
8. Gerenciar as configurações da proteção de objetos compostos:
   - **Verificar arquivos comprimidos**
   - **Verificar pacotes de distribuição**
   - **Verificar arquivos de formatos do Microsoft Office**
   - **Verificar arquivos de formato de e-mail**
9. Selecione a ação a ser executada em objetos infectados e outros objetos detectados:
   - **Desinfectar**
   - **Desinfectar e excluir se a desinfecção falhar**
   - **Excluir**
   - **Recomendado**
   - **Informar**
10. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:
    a. Desmarque ou marque a caixa de seleção **Aplicar a ação aos tipos de objetos selecionados**.
    b. Clique em **Configurações** e selecione os tipos de objetos que serão detectados.

11. Configurar as ações em arquivos compostos que não estejam disponíveis para modificação: desmarque ou marque a caixa de seleção **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado**.

12. No bloco **Exclusões**:

    - Desmarque ou marque a caixa de seleção **Excluir arquivos**.
    - Desmarque ou marque a caixa de seleção **Não detectar objetos por tipos**.

13. No bloco **Adicionar chave**:

    - **Parar a verificação se demorar mais que (s)**
    - **Não verificar objetos compostos com mais de (MB)**
    - **Usar a tecnologia iSwift**
    - **Usar a tecnologia iChecker**

14. Salvar as novas configurações de segurança.

Gerenciar manualmente as configurações de segurança no Console do Aplicativo

1. Na árvore do Console do Aplicativo, expanda o nó **Verificação por demanda**.
2. Selecione o nó 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 de proteção**.
4. Na lista de recursos de arquivos de rede do dispositivo protegido, selecione um item para o qual deseja gerenciar as configurações de segurança.
5. Certifique-se de que o node ou item selecionado seja incluído no escopo da verificação.
6. Clique **Configurar**.
7. Na janela que é aberta, selecione o nível de segurança necessário e clique em **Configurações**..
8. Na guia **Geral**, defina as seguintes configurações:

    - Objetos que devem ser incluídos no escopo de proteção:
        - **Todos os objetos**.
        - **Objetos verificados por formato**.
        - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**.
    - Na seção **Otimização**, marque ou desmarque a caixa de seleção **Proteger somente arquivos novos e modificados**.

- Na seção **Verificação de arquivos compostos**, especifique os objetos compostos que deseja incluir no escopo da verificação:
  - **Verificar arquivos comprimidos**.
  - **Verificar pacotes de distribuição**.
  - **Verificar arquivos de formatos do Microsoft Office**.
  - **Verificar arquivos de formato de e-mail**.

9. Na guia **Ações**, defina as seguintes configurações:
   - Selecione a ação a ser executada em objetos infectados e outros objetos detectados:
     - **Desinfectar**
     - **Desinfectar e excluir se a desinfecção falhar**
     - **Excluir**.
     - **Recomendado**.
     - **Informar**.
   - Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:
     a. Desmarque ou marque a caixa de seleção **Aplicar a ação aos tipos de objetos selecionados**.
     b. Clique em **Configurações** e selecione os tipos de objetos que serão detectados.
   - Configurar as ações em arquivos compostos que não estejam disponíveis para modificação: desmarque ou marque a caixa de seleção **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte o objeto incorporado**.
10. Na guia **Desempenho**, defina as seguintes configurações:
    - No bloco **Exclusões**:
      - Desmarque ou marque a caixa de seleção **Excluir arquivos**.
      - Desmarque ou marque a caixa de seleção **Não detectar objetos por tipos**.

      Clique no botão **Editar** de cada configuração para adicionar exclusões.
    - 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.

11. Salvar as novas configurações de segurança.

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 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. Na árvore do Console do Aplicativo, expanda o nó **Verificação por demanda**.
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 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. Por exemplo, se o Kaspersky Embedded Systems Security detectar um objeto malicioso em cinco arquivos, o valor desse campo aumentará em um.
Objetos infectados e outros	O número de objetos que o Kaspersky Embedded Systems Security 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 não desinfectados	Número de objetos que o Kaspersky Embedded Systems Security não desinfectou pelos seguintes motivos: • O objeto detectado é de um tipo que não pode ser desinfectado. • Ocorreu um erro durante a desinfecção.
Objetos desinfectados	Número de objetos desinfectados pelo Kaspersky Embedded Systems Security.
Objetos removidos	Número de objetos excluídos com sucesso pelo Kaspersky Embedded Systems Security.
Objetos não verificados	Número de objetos no escopo de proteção que o Kaspersky Embedded Systems Security não verificou devido, por exemplo, ao acesso ao objeto estar bloqueado por outro aplicativo.
Arquivos compactados	Número de arquivos compactados verificados pelo Kaspersky Embedded Systems Security.
Objetos compactados	Número de objetos compactados verificados pelo Kaspersky Embedded Systems Security.
Objetos protegidos por senha	Número de objetos (arquivos compactados, por exemplo) que o Kaspersky Embedded Systems Security ignorou porque estavam protegidos por senha.
Objetos corrompidos	Número de objetos ignorados pelo Kaspersky Embedded Systems Security porque seu formato estava corrompido.
Erros de processamento	Número de objetos cujo processamento resultou em um erro.

Campo	Descrição
Objetos não removidos	Número de objetos que o Kaspersky Embedded Systems Security tentou excluir sem sucesso, devido, por exemplo, a um bloqueio no acesso ao objeto por parte de outro aplicativo.
Objetos não processados	Número total de objetos não processados pelo Kaspersky Embedded Systems Security.

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.

Atualização do banco de dados e dos módulos de software do Kaspersky Embedded Systems Security

Esta seção contém informações sobre as tarefas de atualização e reversão de atualização do Kaspersky Embedded Systems Security, além de instruções para a configuração de tarefas.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinaturas de antivírus e atualizações de base de código) pode não estar disponível no software nos EUA.

Atualizar bancos de dados e módulos do software aplicativo

A atualização dos bancos de dados e dos módulos do aplicativo do Kaspersky Embedded Systems Security assegura ao computador a versão de proteção mais recente. No mundo todo, novos tipos de vírus e malware surgem diariamente. Os bancos de dados do Kaspersky Embedded Systems Security contêm informações sobre ameaças e formas de neutralizá-las. Para detectar ameaças rapidamente, é necessário atualizar regularmente os bancos de dados e os módulos do aplicativo.

Atualizações frequentes exigem uma licença em vigor. Se não houver uma licença atual, será possível executar a atualização apenas uma vez.

O Kaspersky Embedded Systems Security baixa atualizações de bancos de dados e módulos do aplicativo a partir dos servidores de atualização HTTP ou FTP da Kaspersky, do Servidor de Administração do Kaspersky Security Center ou de outras fontes de atualização.

É possível baixar 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. Caso gerencie a segurança dos dispositivos de sua organização de forma centralizada com o Kaspersky Security Center, será possível aproveitar o Servidor de Administração para atuar como proxy a fim de baixar atualizações.

Se o processo de download da atualização for interrompido ou resultar em erro, o Kaspersky Embedded Systems Security retornará automaticamente ao uso dos bancos de dados de atualizações instaladas anteriormente. Se os bancos de dados do Kaspersky Embedded Systems Security forem corrompidos, eles podem ser revertidos manualmente para as atualizações instaladas anteriormente.

Ao executar a atualização, os seguintes objetos são baixados e instalados no computador:

- Bancos de dados do Kaspersky Embedded Systems Security. A proteção do computador é fornecida utilizando bancos de dados com assinatura de vírus e outras ameaças e informações sobre a forma de neutralizá-las. Os componentes de proteção usam estas informações quando procuram e neutralizam arquivos infectados no computador. Os bancos de dados são constantemente atualizados com registros de novas ameaças e métodos para neutralizá-las. Portanto, é recomendável fazer a atualização dos bancos de dados regularmente.

  Além dos bancos de dados do Kaspersky Embedded Systems Security, também são atualizadas as unidades de rede que ativam os componentes do aplicativo de interceptação de tráfego de rede.

- Módulos do aplicativo. Além dos bancos de dados do Kaspersky Embedded Systems Security, faça também a atualização dos módulos do programa. A atualização dos módulos do aplicativo soluciona os problemas no Kaspersky Embedded Systems Security relativos a vulnerabilidades neste; adiciona novas funções ou aprimora as existentes.

Durante a atualização, os bancos de dados e os módulos do aplicativo no computador são comparados com a versão mais recente na fonte de atualização. Se forem encontradas diferenças nos bancos de dados e nos módulos do aplicativo, em relação às respectivas versões mais recentes, são instaladas as atualizações que faltam no computador.

Se os bancos de dados estão obsoletos, o pacote de atualização será grande, o que poderá causar tráfego de Internet (uma grande quantidade de MB).

As informações sobre o estado atual dos bancos de dados do Kaspersky Embedded Systems Security são exibidas na janela principal do aplicativo ou na dica de ferramenta visível ao passar o cursor sobre o ícone do aplicativo na área de notificação.

As informações sobre os resultados da atualização e sobre todos os eventos ocorridos durante a execução da tarefa de atualização são registradas no log da tarefa de atualização.

Sobre as tarefas de atualização

O Kaspersky Embedded Systems Security tem duas tarefas de atualização: Atualização e Reversão de atualização.

Por padrão, o Kaspersky Embedded Systems Security se conecta à fonte de atualização a cada hora. É possível configurar todas as tarefas de Atualização, exceto a tarefa de Reversão de atualização. Quando as configurações da tarefa forem modificadas, o Kaspersky Embedded Systems Security aplicará os novos valores na próxima execução da tarefa.

Não é permitido fazer uma pausa e reiniciar as tarefas de atualização.

Atualização

Por padrão, o Kaspersky Embedded Systems Security copia os bancos de dados, e em caso de disponibilidade, os módulos do aplicativo 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 executa a tarefa de Atualização do banco de dados de hora em hora.

Reversão de atualização

A tarefa faz com que o Kaspersky Embedded Systems Security retorne para os bancos de dados e módulos de aplicativos anteriores.

A tarefa Reversão de atualização está desativada por padrão.

Esquemas de atualização do banco de dados e dos módulos de software do Kaspersky Embedded Systems Security

A escolha da fonte na tarefa de atualização depende do esquema de atualização para bancos de dados e módulos de software usados na organização.

Os bancos de dados e módulos do Kaspersky Embedded Systems Security 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 no qual os seguintes aplicativos estejam instalados pode servir como intermediário:

  - Kaspersky Embedded Systems Security (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.

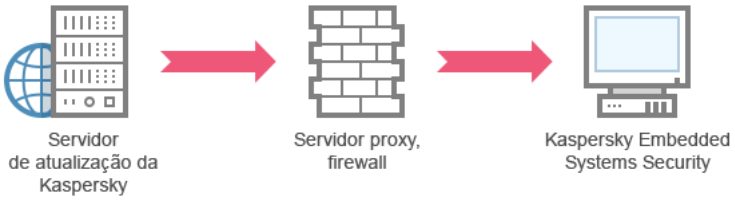
Os esquemas de atualização listados estão descritos abaixo.

Esquema 1. Atualização dos bancos de dados e módulos diretamente da Internet

Para configurar atualizações do Kaspersky Embedded Systems Security diretamente da Internet:

em cada dispositivo protegido nas configurações da tarefa de Atualização do banco de dados, especifique os servidores de atualização da Kaspersky como a fonte de atualização.

Outros servidores HTTPS ou HTTP que têm uma pasta de atualização podem ser configurados como fonte de atualização.



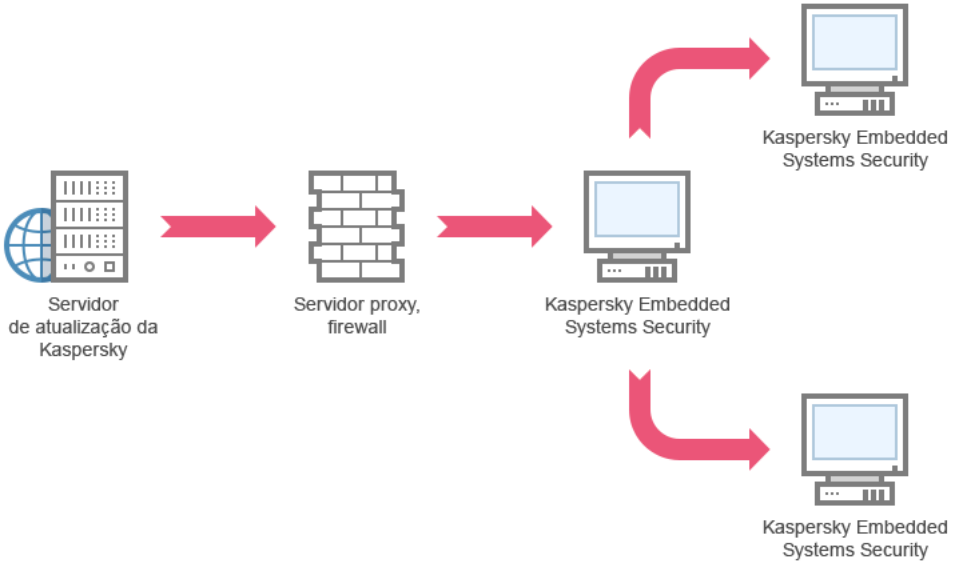
Esquema 1: atualização dos bancos de dados e módulos diretamente da Internet

Esquema 2. Atualização dos bancos de dados e módulos através de um dos dispositivos protegidos

Para configurar o recebimento de atualizações do Kaspersky Embedded Systems Security por meio de um dos dispositivos protegidos:

1. Copie as atualizações para o dispositivo protegido selecionado.
   - Definir as configurações da tarefa da atualização 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:
   - Instale o Agente de rede em cada um dos dispositivos protegidos.
     Para a fonte de atualização, especifique uma pasta na unidade do dispositivo intermediário na qual as atualizações serão baixadas.

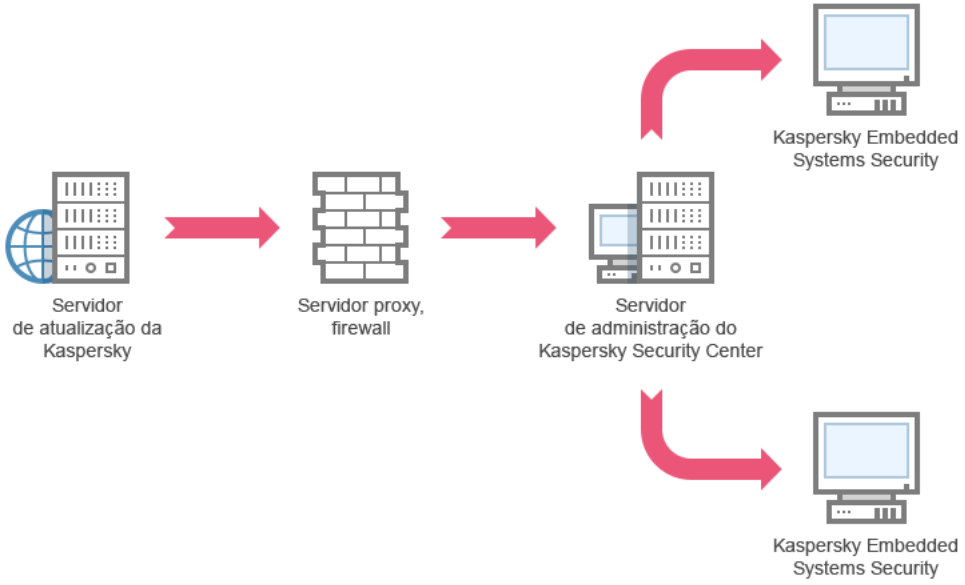
O Kaspersky Embedded Systems Security obterá atualizações através de um dos dispositivos protegidos.



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

Caso esteja usando o Kaspersky Security Center para gerenciar centralmente a proteção antivírus dos dispositivos, baixe as atualizações pelo Servidor de Administração do Kaspersky Security Center instalado em sua rede local.



Esquema 3: atualização dos bancos de dados e módulos pelo Servidor de Administração do Kaspersky Security Center

Para configurar o recebimento de atualizações do Kaspersky Embedded Systems Security por meio do Servidor de Administração do Kaspersky Security Center:

1. Instale o Agente de rede em cada um dos dispositivos protegidos. O Agente de Rede é um componente de software incluído no kit de distribuição do Kaspersky Security Center. Isso garante a interação entre o Servidor de Administração e o Kaspersky Embedded Systems Security 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*.

2. Baixe atualizações dos servidores de atualização da Kaspersky para o Servidor de Administração do Kaspersky Security Center.

   - Configure a tarefa Recuperar atualizações pelo Servidor de administração para o conjunto de dispositivos protegidos especificado.

     Especifique o servidor de atualização da Kaspersky como fonte de atualizações.

3. 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:

   - Instale o Agente de rede em cada um dos dispositivos protegidos.

     a. Especifique o Servidor de Administração do Kaspersky Security Center como a fonte de atualização.

     b. Configure a programação da tarefa se necessário.

O Kaspersky Embedded Systems Security obterá atualizações através do Servidor de Administração do Kaspersky Security Center.

Configurando tarefas de atualização

Como configurar a tarefa de Atualização no Console de Administração do Kaspersky Security Center

1. No Console de Administração do Kaspersky Security Center, vá para a tarefa de atualização local ou de grupo que deseja configurar.
2. Abra a seção **Configurações**.
3. Em **Configurações da atualização para modo local** para o Kaspersky Embedded Systems Security conectado no Servidor de Administração do Kaspersky Security Center, configure as fontes de atualização:
   a. Clique **Configurações**.
      A janela **Atualização de bancos de dados e módulos do aplicativo** é aberta.
   b. Marque as caixas de seleção ao lado das configurações que você deseja editar.
      - Servidor de Administração do Kaspersky Security Center
      - Servidores de atualização Kaspersky

      Caso seja necessário, clique no botão **Adicionar** para adicionar uma fonte de atualização personalizada.
   c. Caso diversas fontes de atualização sejam selecionadas, use os botões **Para cima** e **Para baixo** para definir a prioridade das fontes de atualização. O Kaspersky Embedded Systems Security acessa as fontes de atualização seguindo estritamente a ordem configurada e executa a tarefa de atualização usando o pacote de atualização da primeira fonte de atualização disponível.
      Por padrão, o Kaspersky Embedded Systems Security usa o servidor do Kaspersky Security Center como a primeira fonte de atualização. Isso ajuda a conservar o tráfego durante a atualização. Se uma política não for aplicada ao computador, os servidores da Kaspersky serão selecionados como a primeira fonte de atualização nas configurações da tarefa de Atualização local, pois o aplicativo pode não ter acesso ao Kaspersky Security Center.
   d. Caso tenha selecionado **Servidores de atualização Kaspersky** como fonte de atualização, selecione a ordem que o Kaspersky Embedded Systems Security deve seguir ao selecionar um servidor de atualização da Kaspersky:
      - **Detectar automaticamente**. O aplicativo usa o servidor de atualização Kaspersky mais próximo e disponível.
      - **Selecionar da lista**. O aplicativo usa o servidor de atualização da Kaspersky no país selecionado na lista.
   e. Na janela **Atualização de bancos de dados e módulos do aplicativo**, clique no botão **OK**.
4. Atualização segura do banco de dados do aplicativo
   a. Selecione ou desmarque a caixa de seleção **Baixar atualizações dos bancos de dados do aplicativo**.

b. Selecione ou desmarque a caixa de seleção **Diminuir a carga na E/S de disco**.

c. Caso a caixa de seleção **Diminuir a carga na E/S de disco** seja marcada, especifique a quantidade de memória RAM em megabytes no campo **RAM usada para otimização, 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 640 MB. O tamanho de RAM padrão é 400 MB.

Ao executar a tarefa de Atualização com o recurso de otimização do subsistema de disco ativado, uma das seguintes situações pode acontecer:

- 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. Configurar as atualizações do módulo do software do aplicativo:

a. Selecione ou desmarque a caixa de seleção **Baixar atualizações dos módulos do aplicativo**.

b. Selecione as atualizações dos módulos do aplicativo que deseja instalar.

- **Instalar atualizações críticas e confirmadas**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Embedded Systems Security instalará atualizações críticas automaticamente e todas as outras atualizações do módulo do aplicativo somente depois que a sua instalação for aprovada localmente pela interface do aplicativo ou no lado do Kaspersky Security Center.

- **Instalar somente atualizações confirmadas**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Embedded Systems Security instalará as atualizações somente depois que a sua instalação for aprovada localmente pela interface do aplicativo ou no lado do Kaspersky Security Center. Esta opção é selecionada por padrão.

Se as atualizações do módulo do aplicativo necessitarem da revisão e da aceitação dos termos do Contrato de Licença de Usuário Final, o aplicativo instalará as atualizações depois que os termos do Contrato de Licença de Usuário Final forem aceitos.

6. Configurar a cópia de atualizações em uma pasta para armazenamento local:

a. Selecione ou desmarque a caixa de seleção **Copiar atualizações para uma pasta ou armazenamento local**.

b. Selecionar o conteúdo das atualizações que deseja que o aplicativo copie para a pasta de armazenamento local:

- **Copiar atualizações do banco de dados**. O aplicativo baixa somente as atualizações do banco de dados.
- **Copiar atualizações críticas dos módulos de aplicativo**. O aplicativo baixa somente as atualizações críticas do módulo do aplicativo.
- **Copiar atualizações do banco de dados e atualizações críticas dos módulos do aplicativo**. O aplicativo baixa as atualizações do banco de dados e as atualizações críticas do módulo do aplicativo.

c. Especifique a pasta local ou pasta de rede para a qual o Kaspersky Embedded Systems Security distribuirá as atualizações baixadas.

7. Salvar alterações.

Como configurar a tarefa de Atualização no Console do Aplicativo

1. Na árvore do Console do Aplicativo, abra o nó **Atualização → Atualização de bancos de dados e módulos do aplicativo**.
2. Clique no link **Propriedades** no painel de resultados.

   A janela **Propriedades: Atualização de bancos de dados e módulos do aplicativo** é aberta.
3. Em **Configurações da atualização para modo local** para o Kaspersky Embedded Systems Security conectado no Servidor de Administração do Kaspersky Security Center, configure as fontes de atualização:

   a. Clique **Configurações**.

   A janela **Atualização de bancos de dados e módulos do aplicativo** é aberta.

   b. Marque as caixas de seleção ao lado das configurações que você deseja editar.

   - Servidor de Administração do Kaspersky Security Center
   - Servidores de atualização Kaspersky

   Caso seja necessário, clique no botão **Adicionar** para adicionar uma fonte de atualização personalizada.

   c. Caso diversas fontes de atualização sejam selecionadas, use os botões **Para cima** e **Para baixo** para definir a prioridade das fontes de atualização. O Kaspersky Embedded Systems Security acessa as fontes de atualização seguindo estritamente a ordem configurada e executa a tarefa de atualização usando o pacote de atualização da primeira fonte de atualização disponível.

   Por padrão, o Kaspersky Embedded Systems Security usa o servidor do Kaspersky Security Center como a primeira fonte de atualização. Isso ajuda a conservar o tráfego durante a atualização. Se uma política não for aplicada ao computador, os servidores da Kaspersky serão selecionados como a primeira fonte de atualização nas configurações da tarefa de Atualização local, pois o aplicativo pode não ter acesso ao Kaspersky Security Center.

d. Caso tenha selecionado **Servidores de atualização Kaspersky** como fonte de atualização, selecione a ordem que o Kaspersky Embedded Systems Security deve seguir ao selecionar um servidor de atualização da Kaspersky:

- **Detectar automaticamente**. O aplicativo usa o servidor de atualização Kaspersky mais próximo e disponível.
- **Selecionar da lista**. O aplicativo usa o servidor de atualização da Kaspersky no país selecionado na lista.

e. Na janela **Atualização de bancos de dados e módulos do aplicativo**, clique no botão **OK**.

4. Atualização segura do banco de dados do aplicativo

a. Selecione ou desmarque a caixa de seleção **Baixar atualizações dos bancos de dados do aplicativo**.

b. Selecione ou desmarque a caixa de seleção **Diminuir a carga na E/S de disco**.

c. Caso a caixa de seleção **Diminuir a carga na E/S de disco** seja marcada, especifique a quantidade de memória RAM em megabytes no campo **RAM usada para otimização, 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 640 MB. O tamanho de RAM padrão é 400 MB.

Ao executar a tarefa de Atualização com o recurso de otimização do subsistema de disco ativado, uma das seguintes situações pode acontecer:

- 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. Configurar as atualizações do módulo do software do aplicativo:

a. Selecione ou desmarque a caixa de seleção **Baixar atualizações dos módulos do aplicativo**.

b. Selecione as atualizações dos módulos do aplicativo que deseja instalar.

- **Instalar atualizações críticas e confirmadas**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Embedded Systems Security instalará atualizações críticas automaticamente e todas as outras atualizações do módulo do aplicativo somente depois que a sua instalação for aprovada localmente pela interface do aplicativo ou no lado do Kaspersky Security Center.
- **Instalar somente atualizações confirmadas**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Embedded Systems Security instalará as atualizações somente depois que a sua instalação for aprovada localmente pela interface do aplicativo ou no lado do Kaspersky Security Center. Esta opção é selecionada por padrão.

Se as atualizações do módulo do aplicativo necessitarem da revisão e da aceitação dos termos do Contrato de Licença de Usuário Final, o aplicativo instalará as atualizações depois que os termos do Contrato de Licença de Usuário Final forem aceitos.

6. Configurar a cópia de atualizações em uma pasta para armazenamento local:

   a. Selecione ou desmarque a caixa de seleção **Copiar atualizações para uma pasta ou armazenamento local**.

   b. Selecionar o conteúdo das atualizações que deseja que o aplicativo copie para a pasta de armazenamento local:

   - **Copiar atualizações do banco de dados**. O aplicativo baixa somente as atualizações do banco de dados.
   - **Copiar atualizações críticas dos módulos de aplicativo**. O aplicativo baixa somente as atualizações críticas do módulo do aplicativo.
   - **Copiar atualizações do banco de dados e atualizações críticas dos módulos do aplicativo**. O aplicativo baixa as atualizações do banco de dados e as atualizações críticas do módulo do aplicativo.

   c. Especifique a pasta local ou pasta de rede para a qual o Kaspersky Embedded Systems Security distribuirá as atualizações baixadas.

7. Salvar alterações.

Como configurar a tarefa de Atualização no Kaspersky Security Center Web Console

1. No Web Console, vá para a tarefa de atualização local ou de grupo que deseja configurar.
2. Abra a seção **Configurações**.
3. Selecione a guia **Modo local** para configurar a tarefa de Atualização para o Kaspersky Embedded Systems Security conectado ao Servidor de Administração do Kaspersky Security Center.
4. Configurar as fontes de atualização:

   a. Em **Fontes de atualização**, marque a caixa de seleção ao lado das fontes de atualização que deseja usar:

   - **Servidor de Administração do Kaspersky Security Center**
   - **Servidores de atualização Kaspersky**

   Caso seja necessário, clique no botão **Adicionar** para adicionar uma fonte de atualização personalizada.

b. Caso diversas fontes de atualização sejam selecionadas, use os botões **Para cima** e **Para baixo** para definir a prioridade das fontes de atualização. O Kaspersky Embedded Systems Security acessa as fontes de atualização seguindo estritamente a ordem configurada e executa a tarefa de atualização usando o pacote de atualização da primeira fonte de atualização disponível.

Por padrão, o Kaspersky Embedded Systems Security usa o servidor do Kaspersky Security Center como a primeira fonte de atualização. Isso ajuda a conservar o tráfego durante a atualização. Se uma política não for aplicada ao computador, os servidores da Kaspersky serão selecionados como a primeira fonte de atualização nas configurações da tarefa de Atualização local, pois o aplicativo pode não ter acesso ao Kaspersky Security Center.

5. Atualização segura do banco de dados do aplicativo

a. Selecione ou desmarque a caixa de seleção **Baixar atualizações dos bancos de dados do aplicativo**.

b. Selecione ou desmarque a caixa de seleção **Diminuir a carga na E/S de disco**.

c. Caso a caixa de seleção **Diminuir a carga na E/S de disco** seja marcada, especifique a quantidade de memória RAM em megabytes no campo **RAM usada para otimização, 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 640 MB. O tamanho de RAM padrão é 400 MB.

Ao executar a tarefa de Atualização com o recurso de otimização do subsistema de disco ativado, uma das seguintes situações pode acontecer:

- 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.

6. Configurar as atualizações do módulo do software do aplicativo:

a. Selecione ou desmarque a caixa de seleção **Baixar atualizações dos módulos do aplicativo**.

b. Selecione as atualizações dos módulos do aplicativo que deseja instalar.

- **Instalar atualizações críticas e confirmadas**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Embedded Systems Security instalará atualizações críticas automaticamente e todas as outras atualizações do módulo do aplicativo somente depois que a sua instalação for aprovada localmente pela interface do aplicativo ou no lado do Kaspersky Security Center.

- **Instalar somente atualizações confirmadas**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Embedded Systems Security instalará as atualizações somente depois que a sua instalação for aprovada localmente pela interface do aplicativo ou no lado do Kaspersky Security Center. Esta opção é selecionada por padrão.

Se as atualizações do módulo do aplicativo necessitarem da revisão e da aceitação dos termos do Contrato de Licença de Usuário Final, o aplicativo instalará as atualizações depois que os termos do Contrato de Licença de Usuário Final forem aceitos.

7. Configurar a cópia de atualizações em uma pasta para armazenamento local:

   a. Selecione ou desmarque a caixa de seleção **Copiar atualizações para a pasta**.

   b. Selecionar o conteúdo das atualizações que deseja que o aplicativo copie para a pasta de armazenamento local:

   - **Copiar atualizações do banco de dados**. O aplicativo baixa somente as atualizações do banco de dados.
   - **Copiar atualizações críticas dos módulos de aplicativo**. O aplicativo baixa somente as atualizações críticas do módulo do aplicativo.
   - **Copiar atualizações do banco de dados e atualizações críticas dos módulos do aplicativo**. O aplicativo baixa as atualizações do banco de dados e as atualizações críticas do módulo do aplicativo.

   c. Especifique a pasta local ou pasta de rede para a qual o Kaspersky Embedded Systems Security distribuirá as atualizações baixadas.

8. Salvar alterações.

Atualização SMU do aplicativo

Para atualizar o aplicativo usando o serviço de atualização da Kaspersky (Seamless Update; SMU), você não precisa executar o instalador, ao contrário de outros métodos de atualização. O Kaspersky Embedded Systems Security recebe a nova versão do aplicativo juntamente com os bancos de dados do antivírus da mesma fonte.

Uma atualização do SMU permite atualizar o aplicativo em todos os computadores da sua organização para a versão mais recente. Antes de aplicar uma atualização do SMU, recomendamos testar a nova versão do aplicativo em alguns computadores. Para fazer isso, você deve atualizar o aplicativo nesses computadores manualmente (por exemplo, localmente usando o Assistente de instalação). Não é possível selecionar computadores individuais ao executar uma atualização do SMU.

O agendamento de atualizações do aplicativo é determinado pela equipe da Kaspersky. Para garantir que a nova versão do aplicativo esteja funcionando sem problemas, a Kaspersky disponibiliza atualizações passo a passo. Isso significa que você pode obter sua atualização do SMU até dois meses depois do lançamento de uma nova versão.

É possível gerenciar a atualização do SMU do aplicativo com o uso da tarefa *Atualização de bancos de dados e módulos do aplicativo*. Para que a nova versão do aplicativo seja incluída no mesmo pacote dos bancos de dados do antivírus, é necessário permitir a atualização dos *módulos do aplicativo* nas configurações da tarefa *Atualização de bancos de dados e módulos do aplicativo*.

Etapas de uma atualização do SMU do aplicativo

1. **Após o lançamento de uma nova versão do aplicativo ou de uma atualização de módulo, a Kaspersky distribui a atualização.**
2. **O usuário aprova a atualização do aplicativo.**

   Caso o computador esteja conectado ao Kaspersky Security Center, a atualização estará disponível no Kaspersky Security Center, na seção **Atualizações para os bancos de dados e módulos de software da Kaspersky**. Para obter mais detalhes sobre como aprovar atualizações, consulte a Ajuda do Kaspersky Security Center.

   Caso o computador não esteja conectado ao Kaspersky Security Center, a atualização estará disponível no Console do Aplicativo. Para aprovar a atualização, acesse a seção **Atualização** → **Atualização do aplicativo**, selecione uma versão do aplicativo e, se necessário, aceite os termos e condições dos contratos.
3. **O Kaspersky Embedded Systems Security executa a tarefa Atualização de bancos de dados e módulos do aplicativo de acordo com o agendamento.**

Como resultado, o Kaspersky Embedded Systems Security atualiza o aplicativo no modo "silencioso".

Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security

Antes que as atualizações do banco de dados sejam executadas, o Kaspersky Embedded Systems Security cria cópias de backup dos bancos de dados usados anteriormente. Se uma atualização for interrompida ou resultar em erro, o Kaspersky Embedded Systems Security retornará automaticamente ao uso dos bancos de dados instalados anteriormente.

Caso ocorra algum problema após a atualização dos bancos de dados, será possível reverter às atualizações instaladas anteriormente por meio da tarefa *Reversão da última atualização*.

Para executar a tarefa Reversão da última atualização:

1. Na árvore do Console do Aplicativo, abra a seção **Atualização** → **Reversão da última atualização**.
2. No painel de resultados, clique no link **Iniciar**.

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:

Na árvore do Console do Aplicativo, abra a seção **Atualização** → **Atualização de bancos de dados e módulos do aplicativo**.

No painel de resultados, em **Estatísticas**, é possível encontrar informações sobre a quantidade total de dados obtidos.

Como fazer cópias de backup de objetos

Esta seção fornece informações sobre o backup de objetos maliciosos detectados antes da desinfecção ou exclusão.

Como fazer cópias de backup de objetos. Backup

O Kaspersky Embedded Systems Security salva cópias criptografadas de objetos desinfectados ou excluídos na pasta Backup.

Se o objeto fizer parte de um objeto composto (por exemplo, parte de um arquivo compactado), o Kaspersky Embedded Systems Security salvará o objeto composto inteiro no Backup. Por exemplo, se o Kaspersky Embedded Systems Security 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 podem tornar o sistema lento e reduzir o espaço disponível no disco rígido.

Os arquivos podem ser restaurados do backup para sua pasta original ou para uma pasta diferente no dispositivo protegido. Um arquivo pode ser restaurado do Backup, por exemplo, se um arquivo infectado contiver informações importantes, mas o Kaspersky Embedded Systems Security 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

Esta seção fornece informações sobre a forma de visualizar a lista de arquivos no Backup.

Como visualizar os objetos no Backup no Console de Administração do Kaspersky Security Center

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Adicional** → **Armazenamentos**.
3. Vá para a pasta **Backup**.
4. As informações sobre objetos colocados no Backup são exibidas no painel de resultados do node selecionado.

Como visualizar os objetos de Backup no Kaspersky Security Center Web Console

1. Abrir o Console do Aplicativo.
2. Na árvore do console, selecione **Operações** → **Armazenamentos**.
3. Vá para a pasta **Backup**.
4. As informações sobre objetos colocados no Backup são exibidas no painel de resultados do node selecionado.

Como visualizar os objetos no Backup no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Armazenamentos** → **Backup**.
2. 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 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.

Como classificar os arquivos no Backup no Console de Administração do Kaspersky Security Center

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Adicional** → **Armazenamentos**.
3. Vá para a pasta **Backup**.
4. 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.

Como classificar os arquivos no Backup no Kaspersky Security Center Web Console

1. Abrir o Console do Aplicativo.
2. Na árvore do console, selecione **Operações** → **Armazenamentos**.
3. Vá para a pasta **Backup**.
4. 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.

Como classificar os arquivos no Backup no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Armazenamentos** → **Backup**.
2. 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 um arquivo no Backup, é possível filtrar os arquivos para que a lista exiba apenas os arquivos que satisfaçam os critérios de filtragem (filtros) especificados.

Filtrando os arquivos do Backup no Console de Administração do Kaspersky Security Center

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Suplementar** → **Armazenamentos**.
3. Vá para a pasta **Backup**.
4. No painel direito, clique no link **Nenhum filtro especificado**.
5. Clique em **Ajustar o filtro** e na janela **Configurações de filtragem**, selecione as colunas que serão filtradas.
6. Especifique os operadores e valores para as colunas selecionadas.

7. Os filtros criados serão salvos.
8. Para exibir todos os objetos no Backup novamente, na janela **Configurações de filtragem**, clique em **Limpar tudo**.

Filtrando os arquivos do Backup no Kaspersky Security Center Web Console

1. Abrir o Console do Aplicativo.
2. Na árvore do console, selecione **Operações** → **Armazenamentos**.
3. Vá para a pasta **Backup**.
4. Clique no ícone de filtro e clique no botão **Adicionar** na guia **Filtros**.
5. Selecione uma propriedade que será filtrada.
6. Especifique uma condição e um valor para a propriedade selecionada.
7. Clique **Aplicar**.
   As configurações do Kaspersky Embedded Systems Security são salvas.
8. Para exibir todos os objetos no Backup novamente, na guia **Filtros**, clique em **Limpar tudo**.

Como filtrar os arquivos no Backup no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Armazenamentos** → **Backup**.
2. Na tabela de arquivos, selecione o título da coluna e clique no ícone de filtro no canto superior esquerdo.
3. Configure filtro e clique em **OK**.
   As configurações do Kaspersky Embedded Systems Security são salvas.

Restaurando arquivos do Backup

O Kaspersky Embedded Systems Security 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 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 considere esse arquivo como 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.

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.

Por padrão, quando o Kaspersky Embedded Systems Security restaura um arquivo, ele faz uma cópia desse arquivo no Backup. A cópia do arquivo pode ser excluída do Backup depois de ser restaurada.

Restaurando arquivos do Backup no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Adicional** → **Armazenamentos**.
2. Vá para a pasta **Backup**.
3. Execute uma das seguintes ações:
   - Para restaurar um objeto, selecione **Restaurar** no menu de contexto do nome do objeto.
   - Para restaurar vários objetos, selecione os objetos que deseja restaurar com o uso da tecla CTRL ou SHIFT, clique com o botão direito do mouse em um dos objetos selecionados e selecione **Restaurar** no menu de contexto.
4. Objeto será restaurado para a pasta original.

Restaurando arquivos do Backup no Kaspersky Security Center Web Console

1. Abrir o Console do Aplicativo.
2. Na árvore do console, selecione **Operações** → **Armazenamentos**.
3. Vá para a pasta **Backup**.
4. Selecione objetos da lista e clique no botão **Restaurar**.
5. Objeto será restaurado para a pasta original.

Restaurando arquivos do Backup no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Armazenamentos** → **Backup**.
2. Execute uma das seguintes ações no painel de resultados do node **Backup**:
   - Para restaurar um objeto, selecione **Restaurar** no menu de contexto do objeto que deseja restaurar.
   - Para restaurar vários objetos, selecione os objetos que deseja restaurar com o uso da tecla CTRL ou SHIFT, clique com o botão direito do mouse em um dos objetos selecionados e selecione **Restaurar** no menu de contexto.
3. Na janela **Restaurar 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.

4. Execute uma das seguintes ações:
   - Para restaurar um objeto em seu local original, selecione **Restaurar na pasta de origem**.
   - Para restaurar um objeto para a pasta especificada como a localização de objetos restaurados durante a instalação do aplicativo, 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 requerida ou especifique o caminho para ela.
5. 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).
6. Para aplicar as condições de restauração especificadas ao resto dos objetos selecionados, marque a caixa **Aplicar a todos os objetos selecionados**.
7. Clique **OK**.
8. O Kaspersky Embedded Systems Security 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:
      - **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, marque a caixa de seleção **Aplicar a todos os objetos selecionados** para aplicar a ação selecionada (**Substituir** ou **Renomear**) ao resto dos objetos selecionados. Caso você tenha selecionado **Renomear**, a caixa de seleção **Aplicar a todos os objetos selecionados** estará indisponível.

c. Clique **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 **Restaurar objeto**, a janela **Restaurar objeto** poderá ser aberta novamente. Use essa janela para especificar a localização onde o próximo objeto selecionado será salvo.

Excluindo arquivos do Backup

Excluindo arquivos do Backup no Console de Administração do Kaspersky Security Center

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Adicional** → **Armazenamentos**.
3. Vá para a pasta **Backup**. O painel direito exibe a lista de objetos no Backup.
4. Execute uma das seguintes ações:
   - Para ativar a política, selecione **Excluir** no menu de contexto do aplicativo.
   - Para excluir vários objetos, selecione os objetos que você deseja excluir usando a tecla Ctrl ou Shift, clique com o botão direito do mouse em um dos objetos selecionados e selecione **Excluir** no menu de contexto.
5. Os objetos selecionados serão excluídos do Backup.

Excluindo arquivos do Backup no Kaspersky Security Center Web Console

1. Abrir o Console do Aplicativo.
2. Na árvore do console, selecione **Operações** → **Armazenamentos**.
3. Vá para a pasta **Backup**.
4. Selecione objetos da lista e clique no botão **Excluir**.
5. Os objetos selecionados serão excluídos do Backup.

Removendo arquivos do Backup no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Armazenamentos** → **Backup**.
2. O painel direito exibe a lista de objetos no Backup.
3. Execute uma das seguintes ações:
   - Para ativar a política, selecione **Excluir** no menu de contexto do aplicativo.
   - Para excluir vários objetos, selecione os objetos que você deseja excluir usando a tecla Ctrl ou Shift, clique com o botão direito do mouse em um dos objetos selecionados e selecione **Excluir** no menu de contexto.
4. Os objetos selecionados serão excluídos do Backup.

Envio de objetos possivelmente infectados à Kaspersky para análise

Se o comportamento de um objeto gerar uma suspeita de que ele contém uma ameaça, e se o Kaspersky Embedded Systems Security considerar que o objeto deve ser limpo, talvez você tenha encontrado uma ameaça desconhecida cuja assinatura ainda não foi adicionada ao banco de dados. É possível enviar esse objeto 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 identifique o objeto como infectado e possa desinfectá-lo. Além de poder manter o objeto, você também evitará um surto de vírus.

Para enviar um objeto para análise aos especialistas da Kaspersky no Console de administração do Kaspersky Security Center

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Adicional** → **Armazenamentos**.
3. Vá para a pasta **Backup**.
4. Execute uma das seguintes ações:
   - Para enviar um objeto, selecione **Enviar à Kaspersky** no menu de contexto do nome do objeto.
   - Para enviar vários objetos, selecione os objetos que deseja enviar com o uso da tecla CTRL ou SHIFT, clique com o botão direito do mouse em um dos objetos selecionados e selecione **Enviar à Kaspersky** no menu de contexto.
5. Selecione a pasta para salvar o objeto em seu computador.
6. Depois disso, você receberá a solicitação para acessar o portal do Kaspersky Threat Intelligence e carregar o objeto salvo para obter informações completas sobre ele.

Para enviar um objeto para análise aos especialistas da Kaspersky pelo Kaspersky Security Center Web Console

1. Abrir o Console do Aplicativo.
2. Na árvore do console, selecione **Operações** → **Armazenamentos**.
3. Vá para a pasta **Backup**.
4. Selecione objetos da lista e clique no botão **Enviar à Kaspersky**.
5. Selecione a pasta para salvar o objeto em seu computador.
6. Depois disso, você receberá a solicitação para acessar o portal do Kaspersky Threat Intelligence e carregar o objeto salvo para obter informações completas sobre ele.

O Kaspersky Security Center Web Console ou o Console de Administração não pode ser usado para fazer o envio para a Kaspersky analisar os objetos de Backup caso tenham sido transferidos após a atualização da versão 3.4 ou anterior do aplicativo para a versão 4.0 ou posterior.

Configurando o Backup

Como definir as configurações de backup no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Suplementar** → **Armazenamentos** e clique em **Configurações**.
4. Selecione a guia **Backup**.
5. Especificar as configurações de autenticação
   - **Armazenar objetos por no máximo**
   - **Limitar o tamanho do backup a**
   - **Limitar o valor do espaço disponível para**

     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 o notificará sobre isto enquanto continua colocando objetos no Backup.
6. Salvar alterações.

Como definir as configurações de Backup no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Suplementar** → **Armazenamentos** e clique no botão **Configurar**.
5. Selecione a guia **Backup**.
6. Especificar as configurações de autenticação
   - Armazenar objetos por no máximo
   - Limitar o tamanho do backup a

     Caso o tamanho dos objetos no backup exceda o tamanho máximo do backup, o Kaspersky Embedded Systems Security enviará uma notificação e continuará colocando os objetos simultaneamente no Backup.
7. Salvar alterações.

Como definir as configurações de Backup no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Armazenamentos** → **Backup**.
2. no painel de resultados do node **Backup**, clique no link **Propriedades**.
3. Na janela **Propriedades: Backup**, especifique as configurações de Backup:
   - Armazenar objetos por no máximo
   - Limitar o tamanho do backup a
   - Limitar o valor do espaço disponível para

     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 o notificará sobre isto enquanto continua colocando objetos no Backup.
4. Salvar alterações.

Estatísticas do backup

É possível visualizar informações sobre o status atual do Backup, ou seja, estatísticas do backup.

Para exibir as estatísticas do Backup:

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Armazenamentos** → **Backup**.
2. no painel de resultados do node **Backup**, clique no link **Estatísticas**.

   Isso abre o **Backup.Janela Estatísticas**. A janela **Backup: Estatísticas** 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	Tamanho total dos 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 Contra Ameaças à Rede ou Detecção de Comportamento. 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 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 Contra Ameaças à Rede*: uma atividade típica de ataques à rede é detectada.

  O Kaspersky Embedded Systems Security limpa a lista de bloqueio quando o aplicativo é reiniciado e quando as configurações de proteção contra ameaças à rede são alteradas.

- Para a tarefa de *Detecção de Comportamento*: a criptografia maliciosa de um dispositivo que acessa os recursos de arquivos de 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 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 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 **Editar permissões** para gerenciar o Kaspersky Embedded Systems Security.

Migrando a lista de sessões de rede bloqueadas

Para adicionar sessões de rede que exibem qualquer atividade maliciosa ou criptografada na Lista de sessões de rede bloqueadas e bloquear o acesso aos recursos de arquivos de rede para essas sessões, ao menos um dos seguintes componentes deve ser ativado:

- Proteção Contra Ameaças à Rede
- Detecção de Comportamento

Ativando o bloqueio de hosts não confiáveis no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controle de atividades de rede → Configurações de Proteção Contra Ameaças à Rede** e clique em **Configurações**.
4. Na janela que é aberta, marque a caixa de seleção **Proteção Contra Ameaças à Rede**.
5. Na guia **Geral**, ative a opção **Bloquear**.
6. Marque a caixa de seleção **Bloquear dispositivos de ataque por** e conclua o assistente.
7. Salvar alterações.

Para configurar o bloqueio de sessões de rede não confiáveis para o componente Detecção de Comportamento nas propriedades da política:

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção do Computador em Tempo Real → Detecção de Comportamento** e clique em **Configurações**.
4. Na janela exibida, marque a caixa de seleção **Detecção de Comportamento**.
5. Acesse a guia **Proteção de pastas compartilhadas** e abra a janela **Proteger pastas compartilhadas**.
6. Selecione **Bloquear conexão por** e especifique o tempo de duração do bloqueio.
7. Caso seja necessário, especifique os escopos de proteção e exclusões por endereço IP e máscara.
8. Salvar alterações.

Ativando o bloqueio de hosts não confiáveis no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos) → Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Controle de atividades de rede → Proteção Contra Ameaças à Rede** e clique no botão **Configurar**.
5. Na janela que é aberta, marque a caixa de seleção **Ativar proteção contra ameaças à rede**.
6. Ative o modo **Bloquear**.
7. Marque a caixa de seleção **Bloquear dispositivos de ataque por** e conclua o assistente.
8. Caso seja necessário, especifique as exclusões por endereço IP.
9. Salvar alterações.

Para configurar o bloqueio de sessões de rede não confiáveis para o componente Detecção de Comportamento:

1. Na janela principal do Web Console, selecione **Ativos (dispositivos) → Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.

4. Vá para **Proteção do Computador em Tempo Real** → **Detecção de Comportamento** e clique no botão **Configurar**.
5. Na janela que é aberta, marque a caixa de seleção **Ativar Detecção de Comportamento**.
6. Acesse a guia **Proteção de pastas compartilhadas** e abra a janela **Ativar a proteção de pastas compartilhadas contra criptografia externa**.
7. Selecione **Bloquear conexão** e especifique o tempo de duração do bloqueio na seção **Na detecção de criptografia externa de pastas compartilhadas**.
8. Caso seja necessário, especifique os escopos de proteção e exclusões por endereço IP e máscara.
9. Salvar alterações.

Ativação do bloqueio de hosts não confiáveis no Console do Aplicativo

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Proteção do Computador em Tempo Real** → **Proteção Contra Ameaças à Rede**.
2. no painel de resultados do node **Proteção Contra Ameaças à Rede**, clique no link **Propriedades**.

   A janela **Propriedades: Proteção Contra Ameaças à Rede** é aberta.
3. Na janela que é aberta, marque a caixa de seleção **Proteção Contra Ameaças à Rede**.
4. Na guia **Geral**, ative a opção **Bloquear**.
5. Marque a caixa de seleção **Bloquear dispositivos de ataque por** e conclua o assistente.
6. Salvar alterações.

Para configurar o bloqueio de sessões de rede não confiáveis para o componente Detecção de Comportamento:

1. Na árvore do console do Kaspersky Embedded Systems Security, selecione **Proteção do Computador em Tempo Real** → **Anticryptor**.
2. No painel de resultados do nó **Detecção de Comportamento**, clique em **Propriedades**.
3. Na janela exibida, marque a caixa de seleção **Detecção de Comportamento**.
4. Acesse a guia **Proteção de pastas compartilhadas** e abra a janela **Proteger pastas compartilhadas**.
5. Selecione **Bloquear conexão por** e especifique o tempo de duração do bloqueio.
6. Caso seja necessário, especifique os escopos de proteção e exclusões por endereço IP e máscara.
7. Salvar alterações.

Configurando a lista de sessões bloqueadas no Console do Aplicativo

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Selecione o nó secundário **Sessões de rede bloqueadas**.
3. No painel de resultados, clique no botão **Propriedades**.
4. Na janela que é aberta, marque a caixa de seleção **Bloquear dispositivos de ataque por** e especifique o tempo de duração do bloqueio.
5. Para restaurar o acesso de todas as sessões de rede bloqueadas, clique em **Desbloquear todas** na parte superior da janela.

   Todas as sessões de rede serão removidas da lista e desbloqueadas.
6. Para remover as sessões de rede da lista de sessões de rede bloqueadas, na lista do painel de resultados, selecione uma ou mais sessões e clique em **Desbloquear selecionadas** na parte superior da janela.

   As sessões de rede selecionadas são desbloqueadas.

Registro de eventos. Logs do Kaspersky Embedded Systems Security

Esta seção fornece informações sobre a maneira de trabalhar com os logs do Kaspersky Embedded Systems Security.

Modos para registrar eventos do Kaspersky Embedded Systems Security

Os eventos do Kaspersky Embedded Systems Security são divididos em dois grupos:

- Eventos relacionados à operação de componentes do aplicativo e ao processamento de objetos em tarefas do Kaspersky Embedded Systems Security.
- Os eventos relacionados à administração do Kaspersky Embedded Systems Security, como a inicialização do aplicativo, criação ou exclusão de tarefas ou edição de configurações da tarefa.

O Kaspersky Embedded Systems Security usa os seguintes métodos para registrar eventos em log:

- **Logs de operação dos componentes do aplicativo**. Os logs possuem informações sobre eventos ocorridos durante a operação dos componentes do aplicativo.
- **Log de auditoria do sistema**. O log de auditoria do sistema contém informações sobre eventos relacionados à administração do Kaspersky Embedded Systems Security. Além disso, contém informações sobre eventos associados a violações de segurança ou tentativas de violação de segurança no dispositivo protegido.
- **Log de Eventos**. O log de eventos contém informações sobre eventos requeridos para diagnosticar falhas na operação do Kaspersky Embedded Systems Security. O log de eventos está disponível no Visualizador de Eventos do Microsoft Windows.

Os arquivos que podem ser baixados pelos links a seguir contêm tabelas com as listas completas de eventos do Kaspersky Embedded Systems Security das seguintes categorias:

- Eventos que o Kaspersky Embedded Systems Security grava no log de eventos.

  BAIXAR WEL-EVENTS .ZIP
- Eventos que o Kaspersky Embedded Systems Security envia ao Servidor de Administração.

  BAIXAR KSC-EVENTS.ZIP

Definir as configurações de log

É possível editar as seguintes configurações de logs do Kaspersky Embedded Systems Security:

- 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 armazena arquivos de log de tarefas e o arquivo do log de auditoria do sistema.
- Limites de geração de eventos para *Os bancos de dados estão desatualizados*, *Os bancos de dados estão obsoletos* e *A Verificação de áreas críticas não é realizada há muito tempo*.
- Eventos que o Kaspersky Embedded Systems Security salva em logs de tarefas, no log de auditoria do sistema e no log de eventos do Kaspersky Embedded Systems Security no Visualizador de eventos.
- Configurações para publicar eventos de auditoria e eventos de desempenho de tarefa para o servidor syslog através do protocolo Syslog.

Como definir as configurações de log no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Logs e notificações**.
4. Na seção **Logs de tarefas**, clique no botão **Configurações**.

   A janela **Notificações** é aberta.
5. Nesta janela, selecione o log que deseja configurar e especifique as configurações de eventos individuais:
   - Onde os eventos são salvos: relatório local ou Log de eventos do Windows.
   - Notificações de eventos: Notificar por e-mail, Notificar usando o serviço de terminal e/ou Notificar executando o arquivo executável.
   - Caso deseje enviar o evento para um servidor SIEM e/ou para o Kaspersky Security Center.
6. Configure os limites de geração de eventos clicando em **Configurações dos limites de geração de eventos**.
7. Isso abre uma janela; nessa janela, especifique o número de dias após os quais os seguintes eventos devem ser registrados: *Os bancos de dados estão desatualizados*, *Os bancos de dados estão obsoletos* e *A Verificação de áreas críticas não é realizada há muito tempo*.
8. Configure a conexão do servidor SIEM clicando em **Configurações de notificação SIEM**.
9. Configure as notificações por e-mail clicando em **Configurações de notificação por e-mail**.
10. Salvar alterações.

Como definir as configurações de log no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Logs e notificações** → **Logs de tarefas** e clique no botão **Configurar**.
5. Isso abre uma janela; nessa janela, na guia **Notificações**, selecione o log que deseja configurar e especifique as configurações para eventos individuais:
   - Onde os eventos são salvos: relatório local ou Log de eventos do Windows.
   - Notificações de eventos: Notificar por e-mail, Notificar usando o serviço de terminal e/ou Notificar executando o arquivo executável.
   - Caso deseje enviar o evento para um servidor SIEM e/ou para o Kaspersky Security Center.
6. Configure as notificações por e-mail na guia **Configurações de notificação por e-mail**.
7. Configure a conexão do servidor SIEM na guia **Integração SIEM**.
8. Salvar alterações.

Como definir as configurações de log no Console do Aplicativo:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Registros e notificações**.
2. Selecione **Propriedades**.

   A janela **Notificações** é aberta.
3. Nesta janela, selecione o log que deseja configurar e especifique as configurações de eventos individuais:
   - Onde os eventos são salvos: relatório local ou Log de eventos do Windows.
   - Notificações de eventos: Notificar por e-mail, Notificar usando o serviço de terminal e/ou Notificar executando o arquivo executável.
   - Caso deseje enviar o evento para um servidor SIEM e/ou para o Kaspersky Security Center.
4. Configure os limites de geração de eventos clicando em **Configurações dos limites de geração de eventos**.
5. Isso abre uma janela; nessa janela, especifique o número de dias após os quais os seguintes eventos devem ser registrados: *Os bancos de dados estão desatualizados (dias)*, *Os bancos de dados estão obsoletos (dias)* e *A Verificação de áreas críticas não é executada há muito tempo (dias)*.
6. Configure a conexão do servidor SIEM clicando em **Configurações de notificação SIEM**.

7. Configure as notificações por e-mail clicando em **Configurações de notificação por e-mail**.

8. Salvar alterações.

Classificação de eventos no log

Por padrão, os eventos no log são exibidos em ordem cronológica inversa.

Para classificar eventos no log:

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Logs e notificações**.
2. Selecione o log desejado.
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.

Filtragem de eventos no log

É possível configurar o log para exibir somente os registros de eventos que satisfaçam as condições de filtragem (filtros) especificadas.

Para filtrar eventos no log:

1. Na árvore do Console do Aplicativo, expanda o nó **Registros e notificações**.
2. Selecione o log para o qual deseja configurar um filtro e, no painel de resultados, clique em **Filtrar**.

   A janela **Configurações de filtro** é aberta.
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 **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 **OK** para salvar as condições de filtragem dos eventos de log.

   A lista de eventos do log exibe somente os eventos que atendem às condições do filtro. Os resultados filtrados serão salvos para a próxima vez que você visualizar o log.

Para desativar o filtro:

1. Na árvore do Console do Aplicativo, expanda o nó **Registros e notificações**.
2. Selecione o log para o qual deseja remover um filtro e clique em **Remover filtro**.

   O log exibirá todos os eventos.

Exclusão de eventos do log

Por padrão, o Kaspersky Embedded Systems Security retém os registros de log por 30 dias. É possível alterar o período de armazenamento de registros em um log.

Para excluir eventos do log:

1. Na árvore do Console do Aplicativo, expanda o nó **Registros e notificações**.
2. Selecione o log do qual deseja excluir eventos e, no painel de resultados, clique em **Limpar**.
3. Confirme a operação de limpeza.

   O log é limpo.

Exportação de informações do log

É possível exportar dados de logs para um arquivo CSV ou TXT.

Para exportar eventos de logs:

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Selecione um log e, no painel de resultados, clique no botão **Exportar logs**.

   A janela **Salvar como** é aberta.

3. Especifique o nome, a localização e o tipo do arquivo para o qual deseja exportar dados do log.
4. Clique **Salvar**.

   As informações dos logs são salvas no arquivo especificado.

Log de auditoria do sistema

O Kaspersky Embedded Systems Security executa uma auditoria de sistema de eventos relacionados à administração do Kaspersky Embedded Systems Security. O aplicativo registra informações sobre o início do aplicativo, os inícios e interrupções de tarefas do Kaspersky Embedded Systems Security, alterações nas configurações da tarefa, criação e exclusão de tarefas de Verificação por Demanda. O aplicativo também registra informações sobre eventos associados a violações de segurança ou tentativas de violação de segurança no dispositivo protegido. Os registros desses eventos são exibidos no painel de resultados ao selecionar o nó **Auditoria do Sistema** no Console do Aplicativo.

Por padrão, o Kaspersky Embedded Systems Security armazena registros no log de auditoria do sistema por 30 dias. É possível alterar o período de armazenamento de registros em um log.

É possível especificar uma pasta que será usada pelo Kaspersky Embedded Systems Security para armazenar arquivos contendo o log de auditoria do sistema diferentes da pasta padrão.

Logs de tarefas

As informações sobre a operação dos componentes e tarefas do Kaspersky Embedded Systems Security são exibidas no Console do Aplicativo no painel de resultados quando o usuário seleciona um nó com o nome do componente ou da tarefa na seção **Registros e notificações**.

O Kaspersky Embedded Systems Security tem como padrão manter os registros nos logs de componentes e tarefas por 30 dias. No caso de tarefas é a partir de sua conclusão. É possível alterar o período de armazenamento de registros em logs de tarefas e de componentes.

É possível definir uma pasta diferente da padrão para o Kaspersky Embedded Systems Security armazenar os arquivos de log de tarefas e componentes. Você também pode selecionar os eventos que o Kaspersky Embedded Systems Security registra nos logs de tarefas e componentes.

Visualizando estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security 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:

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Selecione uma tarefa e, no painel de resultados, selecione a guia **Estatísticas**.

Visualizando o log de eventos do Kaspersky Embedded Systems Security no Visualizador de eventos

É possível visualizar o log de eventos do Kaspersky Embedded Systems Security 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 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:

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 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 nó **Visualizador de Eventos** aparece.

6. Expanda o nó **Visualizador de Eventos** e selecione o nó secundário **Logs de Aplicativos e Serviços** > **Kaspersky Embedded Systems Security**.

O log de evento do Kaspersky Embedded Systems Security é exibido.

Sobre a integração SIEM

Para reduzir a carga em 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 tarefas 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 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.

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.

É possível reduzir o risco dos eventos não serem enviados ao servidor SIEM por meio da configuração de conexões com vários servidores SIEM.

O Kaspersky Embedded Systems Security estabelecerá conexão com o primeiro servidor da SIEM na lista. Caso uma tentativa de conexão falhe, o Kaspersky Embedded Systems Security tentará se conectar a outros servidores da lista, um por um.

O Kaspersky Embedded Systems Security 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.

Como configurar a integração SIEM no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Selecione a seção **Registros e notificações**.
4. No bloco **Integração SIEM**, clique no botão **Configurações**.

   A janela **Integração SIEM** é aberta.
5. No bloco **Configurações de integração**, marque a caixa de seleção **Ativar transmissão de eventos de segurança para um servidor SIEM**.

6. Configure a conexão do servidor SIEM no bloco **Configurações de conexão com servidores SIEM**:

    a. Clique **Adicionar**.

    b. Isso abre a janela **Adicionar servidor**; nessa janela, insira o endereço do servidor SIEM (IPv4, DNS), a porta e o protocolo de conexão.

    c. Clique **Configurações de segurança da conexão TCP**.

    d. Isso abre a janela **Configurações de segurança da conexão TCP**; nessa janela, gerencie as configurações de conexão do servidor SIEM (consulte a tabela abaixo).

7. Caso seja necessário, marque a caixa de seleção **Remover as cópias locais para os eventos que foram enviados para um servidor de syslog remoto** no bloco **Configurações de exportação de eventos para um servidor SIEM**. Se a caixa de seleção for marcada, o aplicativo exclui cópias locais de eventos depois que eles tiverem sido publicados com sucesso no servidor SIEM. Este modo é recomendado em dispositivos com desempenho limitado. Se a caixa de seleção for desmarcada, o aplicativo apenas enviará os eventos para o servidor SIEM. As cópias de logs continuam sendo armazenadas localmente. Por padrão, a caixa de seleção fica desmarcada.

    O aplicativo nunca exclui versões locais do log de segurança.

8. No bloco **Formato de eventos**, selecione o formato para o qual deseja converter eventos do aplicativo para que sejam enviados ao servidor SIEM. A opção **Converter os eventos para DADOS ESTRUTURADOS** é selecionada por padrão. Recomendamos selecionar o formato de eventos com base na configuração do servidor SIEM utilizado.

9. Feche o cadeado para aplicar a política aos computadores.

10. Clique no botão **OK** para salvar as alterações.

Como configurar a integração SIEM no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

    A janela de propriedades da política é exibida.

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

4. Selecione a seção **Logs e notificações**.

5. No bloco **Integração SIEM**, clique no botão **Configurar**.

    A janela **Integração SIEM** é aberta.

6. Marque a caixa de seleção **Ativar transmissão de eventos de segurança para um servidor SIEM**.

7. Configure a conexão do servidor SIEM no bloco **Configurações de conexão com servidores SIEM**:

   a. Clique **Adicionar**.

   b. Isso abre a janela **Servidor SIEM**; nessa janela, insira o endereço do servidor SIEM (IPv4, DNS), a porta e o protocolo de conexão.

   c. No bloco **Proteção de conexão**, clique no link **Configurações de conexão com servidores SIEM**.

   d. Isso abre a janela **Configurações de conexão com servidores SIEM**; nessa janela, gerencie as configurações de conexão do servidor SIEM (consulte a tabela abaixo).

   e. No bloco **Formato de eventos**, selecione o formato para o qual deseja converter eventos do aplicativo para que sejam enviados ao servidor SIEM. A opção **Converter os eventos para DADOS ESTRUTURADOS** é selecionada por padrão. Recomendamos selecionar o formato de eventos com base na configuração do servidor SIEM utilizado.

   f. Caso seja necessário, marque a caixa de seleção **Remover as cópias locais para os eventos que foram enviados para um servidor de syslog remoto** no bloco **Configurações de conexão**. Se a caixa de seleção for marcada, o aplicativo exclui cópias locais de eventos depois que eles tiverem sido publicados com sucesso no servidor SIEM. Este modo é recomendado em dispositivos com desempenho limitado. Se a caixa de seleção for desmarcada, o aplicativo apenas enviará os eventos para o servidor SIEM. As cópias de logs continuam sendo armazenadas localmente. Por padrão, a caixa de seleção fica desmarcada.

      O aplicativo nunca exclui versões locais do log de segurança.

8. Feche o cadeado para aplicar a política aos computadores.

9. Clique no botão **OK** para salvar as alterações.

Como configurar a integração SIEM no Console do Aplicativo

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Registros e notificações**.

2. Selecione **Integração SIEM**.

   A janela **Integração SIEM** é aberta.

3. No bloco **Configurações de integração**, marque a caixa de seleção **Ativar transmissão de eventos de segurança para um servidor SIEM**.

4. Configure a conexão do servidor SIEM no bloco **Configurações de conexão com servidores SIEM**:

   a. Clique **Adicionar**.

   b. Isso abre a janela **Adicionar servidor**; nessa janela, insira o endereço do servidor SIEM (IPv4, DNS), a porta e o protocolo de conexão.

   c. Clique **Configurações de segurança da conexão TCP**.

   d. Isso abre a janela **Configurações de segurança da conexão TCP**; nessa janela, gerencie as configurações de conexão do servidor SIEM (consulte a tabela abaixo).

5. Caso seja necessário, marque a caixa de seleção **Remover as cópias locais para os eventos que foram enviados para um servidor de syslog remoto** no bloco **Configurações de exportação de eventos para um servidor SIEM**. Se a caixa de seleção for marcada, o aplicativo exclui cópias locais de eventos depois que eles tiverem sido publicados com sucesso no servidor SIEM. Este modo é recomendado em dispositivos com desempenho limitado. Se a caixa de seleção for desmarcada, o aplicativo apenas enviará os eventos para o servidor SIEM. As cópias de logs continuam sendo armazenadas localmente. Por padrão, a caixa de seleção fica desmarcada.

   O aplicativo nunca exclui versões locais do log de segurança.

6. No bloco **Formato de eventos**, selecione o formato para o qual deseja converter eventos do aplicativo para que sejam enviados ao servidor SIEM. A opção **Converter os eventos para DADOS ESTRUTURADOS** é selecionada por padrão. Recomendamos selecionar o formato de eventos com base na configuração do servidor SIEM utilizado.

7. Clique no botão **OK** para salvar as alterações.

Configurações de conexão do servidor SIEM

Parâmetro	Descrição
Tempo limite (s)	Tempo limite máximo de resposta do servidor da SIEM. Quando o tempo limite se esgotar, o Kaspersky Embedded Systems Security tenta estabelecer conexão com um servidor da SIEM diferente.
Certificado TLS do servidor	Certificado TLS para estabelecer uma conexão confiável com o servidor da SIEM. É possível obter um certificado TLS com o uso da interface de gerenciamento SIEM.
Usar autenticação bidirecional	Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Embedded Systems Security e a SIEM. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do SIEM, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um contêiner criptográfico é um arquivo comprimido PFX com um certificado e uma chave privada. Depois de definir as configurações do SIEM, é necessário ativar a autenticação bidirecional nas configurações do Kaspersky Embedded Systems Security com o uso de uma caixa de seleção e com o carregamento de um contêiner criptográfico protegido por senha. O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

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 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.

As notificações de administrador ou usuário podem ser ativadas usando vários métodos:

- 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.

- Executando um arquivo executável.

  Esse método executa um arquivo executável armazenado na unidade local do dispositivo protegido quando um evento ocorre.

- 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.

Como configurar notificações de eventos no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Logs e notificações**.
4. Na seção **Logs de tarefas**, clique no botão **Configurações**.

   A janela **Notificações** é aberta.
5. Selecione o evento para o qual deseja selecionar um método de notificação e clique em **Configurações de notificação**.

   A janela **Configurações de notificação** é aberta.
6. Para uma notificação por e-mail, na guia **E-mail**, é possível adicionar o texto da mensagem de notificação de evento.

   Para adicionar campos com informações sobre um evento, clique no botão **Variável** e selecione os campos relevantes na lista suspensa. Os campos com informações do evento estão descritos na tabela nesta seção.

   Para restaurar o texto padrão da mensagem de evento, clique no botão **Por padrão**.
7. Para uma notificação executando 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.
8. Para uma notificação usando o serviço do terminal, na guia **Serviço do terminal**, é possível adicionar o texto da mensagem de notificação de evento.

   Para adicionar campos com informações sobre um evento, clique no botão **Variável** e selecione os campos relevantes na lista suspensa. Os campos com informações do evento estão descritos na tabela nesta seção.

Para restaurar o texto padrão da mensagem de evento, clique no botão **Por padrão**.

9. Salvar alterações.

Como configurar notificações de eventos no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Logs e notificações** → **Logs de tarefas** e clique no botão **Configurar**.
5. Isso abre uma janela; nessa janela, clique no evento para o qual deseja selecionar um método de notificação.

   A janela **Configurações de notificação** é aberta.
6. Para uma notificação por e-mail, na seção **Notificar usuários**, marque a caixa de seleção **Enviando e-mail** e adicione o texto da mensagem de notificação de evento.

   Para adicionar campos com informações sobre um evento, clique no botão **Adicionar variável** e selecione os itens relevantes da lista. Os campos com informações do evento estão descritos na tabela nesta seção.

   Para restaurar o texto padrão da mensagem de evento, clique no botão **Reiniciar**.
7. Para uma notificação executando um arquivo executável, na seção **Notificar administradores**, marque a caixa de seleção **Executando o arquivo executável** e insira o caminho completo para um arquivo em um disco local do dispositivo protegido. 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.
8. Para uma notificação usando o serviço de terminal, na seção **Notificar administradores**, marque a caixa de seleção **Usando o serviço de terminal** e adicione o texto da mensagem de notificação de evento.

   Para adicionar campos com informações sobre um evento, clique no botão **Adicionar variável** e selecione os itens relevantes da lista. Os campos com informações do evento estão descritos na tabela nesta seção.

   Para restaurar o texto padrão da mensagem de evento, clique no botão **Reiniciar**.
9. Salvar alterações.

Como configurar notificações de eventos no Console do Aplicativo

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Registros e notificações**.
2. Selecione **Propriedades**.

   A janela **Notificações** é aberta.

3. Selecione o evento para o qual deseja selecionar um método de notificação e clique em **Configurações de notificação**.

   A janela **Configurações de notificação** é aberta.

4. Para uma notificação por e-mail, na guia **E-mail**, é possível adicionar o texto da mensagem de notificação de evento.

   Para adicionar campos com informações sobre um evento, clique no botão **Variável** e selecione os campos relevantes na lista suspensa. Os campos com informações do evento estão descritos na tabela nesta seção.

   Para restaurar o texto padrão da mensagem de evento, clique no botão **Por padrão**.

5. Para uma notificação executando 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.

6. Para uma notificação usando o serviço do terminal, na guia **Serviço do terminal**, é possível adicionar o texto da mensagem de notificação de evento.

   Para adicionar campos com informações sobre um evento, clique no botão **Variável** e selecione os campos relevantes na lista suspensa. Os campos com informações do evento estão descritos na tabela nesta seção.

   Para restaurar o texto padrão da mensagem de evento, clique no botão **Por padrão**.

7. Salvar alterações.

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 devolve ao detectar um objeto. Você pode 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 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 e Proteção de Armazenamento em Rede-RPC, o nome do dispositivo protegido do usuário que acessou o objeto no dispositivo.
%USER_NAME%	Nas tarefas Proteção de Arquivos em Tempo Real e Proteção de Armazenamento em Rede-RPC, 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).
%PROTOCOL%	O protocolo sendo usado.

Variável	Descrição
%MESSAGE%	Texto da mensagem.
%DEVICE_INSTANCEPATH%	Caminho para a instância do dispositivo.
%DEVICE_VID%	ID do fornecedor do dispositivo.
%DEVICE_PID%	Tipo do controlador.
%DEVICE_SERIALNUMBER%	Número de série do dispositivo.

Configuração de notificações por e-mail

Como configurar notificações por e-mail no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Logs e notificações**.
4. Na seção **Logs de tarefas**, clique no botão **Configurações**.
   A janela **Notificações** é aberta.
5. Clique **Configurações de notificação por e-mail**.
6. Na janela que é aberta, marque a caixa de seleção **Enviar notificações de evento**.
7. Em **Enviar notificação em nome de**, especifique as informações do remetente: endereço do remetente, servidor SMTP, porta do servidor SMTP, nome de usuário e senha.
8. Em **Destinatário da notificação**, especifique o endereço de e-mail do destinatário.
9. Especifique o modo de envio: **Se ocorrerem eventos** ou **Por agendamento (agendamento não especificado)**. Para configurar o agendamento, clique em **Editar**.
10. Salvar alterações.

Como configurar notificações por e-mail no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Vá para **Logs e notificações** → **Logs de tarefas** e clique no botão **Configurar**.
5. Uma janela será aberta; nessa janela, selecione a guia **Configurações de notificação por e-mail**.

6. Marque a caixa de seleção **Enviar notificações de evento**.
7. Especifique as informações do remetente: endereço do remetente, servidor SMTP, porta do servidor SMTP, nome de usuário e senha.
8. Especifique o endereço de e-mail do destinatário.
9. Especifique o modo de envio: **Se ocorrerem eventos** ou **Por agendamento**. Se aplicável, configure o agendamento.
10. Salvar alterações.

Como configurar notificações por e-mail no Console do Aplicativo

1. Na árvore do Console do Aplicativo, abra o menu de contexto do node **Registros e notificações**.
2. Selecione **Propriedades**.

   A janela **Notificações** é aberta.
3. Clique **Configurações de notificação por e-mail**.
4. Na janela que é aberta, marque a caixa de seleção **Enviar notificações de evento**.
5. Em **Enviar notificação em nome de**, especifique as informações do remetente: endereço do remetente, servidor SMTP, porta do servidor SMTP, nome de usuário e senha.
6. Em **Destinatário da notificação**, especifique o endereço de e-mail do destinatário.
7. Especifique o modo de envio: **Se ocorrerem eventos** ou **Por agendamento (agendamento não especificado)**. Para configurar o agendamento, clique em **Editar**.
8. Salvar alterações.

Configuração de interações com o Servidor de Administração

É necessário selecionar os tipos de objetos sobre os quais o Kaspersky Embedded Systems Security envia informações ao Servidor de Administração do Kaspersky Security Center.

Como configurar a integração com o Servidor de Administração no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na seção **Logs e notificações**, clique no botão **Configurações** na subseção **Interação com o Servidor de Administração**.

4. Isso abre uma janela; nessa janela, escolha os tipos de objetos sobre os quais o Kaspersky Embedded Systems Security enviará informações ao Servidor de Administração do Kaspersky Security Center:

   - **Sobre os arquivos no Backup**
   - **Sobre os arquivos não processados**
   - **Sobre os dispositivos instalados**
   - **Sobre uma cadeia de desenvolvimento de ameaças**

5. Salvar alterações.

   O Kaspersky Embedded Systems Security enviará informações sobre os tipos de objetos selecionados para o Servidor de Administração.

Como configurar a interação com o Servidor de Administração no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Na seção **Logs e notificações**, clique no botão **Configurar** na subseção **Interação com o Servidor de Administração**.

5. Isso abre uma janela; nessa janela, escolha os tipos de objetos sobre os quais o Kaspersky Embedded Systems Security enviará informações ao Servidor de Administração do Kaspersky Security Center:

   - **Arquivos em backup**
   - **Sobre os arquivos não processados**
   - **Sessões de rede bloqueadas**
   - **Dispositivos e redes Wi-Fi**

6. Salvar alterações.

Managed Detection and Response

O Kaspersky Embedded Systems Security é compatível com a integração da solução Managed Detection and Response.

O Kaspersky Managed Detection and Response (MDR) oferece proteção contínua contra o crescente volume de ameaças que contornam as defesas automatizadas, sendo ideal para organizações com escassez de especialistas, profissionais qualificados ou recursos internos limitados. Diferentemente de ofertas semelhantes no mercado, este serviço se baseia em um histórico comprovado de pesquisas eficazes sobre ataques direcionados para garantir proteção contínua, inclusive contra as ameaças mais complexas. O serviço aumenta a resiliência da empresa contra ameaças cibernéticas e, ao mesmo tempo, permite que seus recursos se dediquem a outras atividades.

O MDR usa dados de telemetria recebidos de endpoints e aprendizado de máquina. O MDR envia dados do incidente aos especialistas da Kaspersky. Os especialistas podem então processar o incidente e, por exemplo, adicionar uma nova entrada aos bancos de dados antivírus. Como alternativa, os especialistas podem emitir recomendações sobre o processamento do incidente e, por exemplo, sugerir o isolamento do computador da rede. Para obter informações detalhadas sobre como a solução funciona, consulte a Ajuda do Kaspersky Managed Detection and Response.

Configurações de integração MDR

O Kaspersky Managed Detection and Response requer ativar o modo estendido do componente Kaspersky Security Network. Caso contrário, o Kaspersky Managed Detection and Response não receberá os dados de telemetria necessários para a operação adequada.

Para o Kaspersky Managed Detection and Response trabalhar com o Servidor de Administração por meio do Kaspersky Security Center Web Console, também é preciso estabelecer uma nova conexão segura, uma *conexão em segundo plano*. O Kaspersky Managed Detection and Response solicita ao usuário estabelecer uma conexão em segundo plano quando a solução for implementada. Certifique-se de que a conexão em segundo plano esteja estabelecida.

Estabelecimento de uma conexão em segundo plano no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Configurações** → **Integração**.
2. Ir para a seção **Integração**.
3. Ative o botão de alternância **Conexão em segundo plano para integração Ativado**.
4. Salvar alterações.

A integração com o Kaspersky Managed Detection and Response compreende as seguintes etapas:

1. **Instalação do componente Managed Detection and Response**

   Para a integração do Kaspersky Embedded Systems Security com a solução Managed Detection and Response, o componente Managed Detection and Response é usado. Para instalar o componente, acesse as configurações do pacote de instalação, o Assistente de Instalação ou o Painel de Controle do Windows e, na etapa de seleção de componentes, escolha **Managed Detection and Response**.

2 Configuração da Kaspersky Private Security Network

A partir da atualização de julho de 2025, a solução Managed Detection and Response passa a ser compatível com a operação sem o arquivo de configuração da KPSN. Para obter informações detalhadas sobre como a solução MDR usa a Kaspersky Security Network, consulte a Ajuda do Kaspersky Managed Detection and Response.

Se a sua configuração não atender aos requisitos para execução sem arquivos de configuração da KPSN, carregue o arquivo de configuração da KPSN nas propriedades do Servidor de Administração. O arquivo de configuração da KPSN está localizado no arquivo ZIP do arquivo de configuração do MDR. Você também pode **carregar o arquivo de configuração da KPSN por meio da linha de comando**.

1. No dispositivo, execute um interpretador de linha de comando (por exemplo, cmd.exe) com permissões de administrador local.
2. Usando o comando `cd`, navegue até a pasta onde o arquivo kavshell.exe está localizado.

   Por exemplo, `cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0` e pressione **ENTER**.

   Você também pode adicionar o caminho do executável à variável de sistema %PATH% durante a fase de instalação do aplicativo e executar o comando sem precisar navegar até a pasta do aplicativo.
3. Execute o seguinte comando:

   ```
   KAVSHELL KSN [/global] [/private <caminho completo para o arquivo de configuração da KSN Privada>] [/login=<nome da conta de usuário atual>] [/pwd=<senha de /login ou senha do KLAdmin caso /login não seja especificado>]
   ```

   Exemplo:

   ```
   KAVSHELL KSN /private C:\kpsn_config.pkcs7
   ```

Para obter detalhes sobre a configuração da Kaspersky Security Network, consulte a ajuda do Kaspersky Security Center.

3 Ativação do Kaspersky Managed Detection and Response

Para ativar a solução Managed Detection and Response no Kaspersky Embedded Systems Security, é necessária uma licença separada para o Kaspersky Managed Detection and Response for Embedded Systems Security Add-on. Para obter informações detalhadas sobre a ativação da solução, consulte a Ajuda do Kaspersky Managed Detection and Response.

O Kaspersky Embedded Systems Security não oferece suporte a arquivos de configuração do MDR (arquivos BLOB). Todos os ativos serão colocados no locatário raiz.

4 Ativação do componente Managed Detection and Response

Como ativar o componente Managed Detection and Response no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Selecione a seção **Servidores de coleta de telemetria**.

4. No bloco **Managed Detection and Response**, clique no botão **Configurações**.

   A janela **Managed Detection and Response** é aberta.

5. Marque a caixa de seleção **Managed Detection and Response**.

6. Salvar alterações.

Como ativar o componente Managed Detection and Response no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.

2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.

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

4. Selecione a seção **Servidores de coleta de telemetria**.

5. No bloco **Managed Detection and Response**, clique no botão **Configurações**.

   A janela **Managed Detection and Response** é aberta.

6. Marque a caixa de seleção **Managed Detection and Response DESATIVADO**.

7. Salvar alterações.

Como ativar o componente Managed Detection and Response no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o node **Servidores de coleta de telemetria** → **Managed Detection and Response**.

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

   A janela **Managed Detection and Response** é exibida na guia **Geral**.

3. Marque a caixa de seleção **Managed Detection and Response**.

4. Salvar alterações.

Como ativar o componente Managed Detection and Response a partir da linha de comando

1. No dispositivo, execute um interpretador de linha de comando (por exemplo, cmd.exe) com permissões de administrador local.

2. Usando o comando `cd`, navegue até a pasta onde o arquivo kavshell.exe está localizado.

   Por exemplo, `cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0` e pressione **ENTER**.

   Você também pode adicionar o caminho do executável à variável de sistema %PATH% durante a fase de instalação do aplicativo e executar o comando sem precisar navegar até a pasta do aplicativo.

3. Execute o seguinte comando:

```
KAVSHELL MDR /<enable|disable|show> [/login:<nome da conta de usuário atual>]
[/pwd:<senha de /login ou senha do KLAdmin caso /login não seja
especificado>]
```

Parâmetros de comando para ativar o Managed Detection and Response

Parâmetro	Descrição
`MDR /<enable|disable|show>`	Argumento necessário. Permite ativar, desativar e visualizar o status do Managed Detection and Response
`/LOGIN=<nome da conta do usuário>`	Argumento opcional. Permite especificar o nome da conta de usuário com permissões suficientes. Se essa opção não for especificada, o aplicativo solicitará o nome de usuário na próxima linha. Não é necessário informar esse valor se você tiver informado a senha do KLAdmin.
`/PWD=<senha de /login ou senha do KLAdmin caso /login não seja especificado>`	Permite especificar a senha da conta de usuário KLAdmin ou de uma conta de usuário com permissões suficientes. Se essa opção não for especificada, o aplicativo solicitará a senha na próxima linha.

Entrar 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

Caso não possa encontrar uma solução para o seu problema na documentação do aplicativo ou em uma das fontes de informação sobre o Kaspersky Embedded Systems Security, recomendamos entrar em contato com o Suporte Técnico. Os especialistas do Suporte Técnico responderão as suas perguntas sobre a instalação e o uso do Kaspersky Embedded Systems Security.

O Kaspersky oferece suporte ao Kaspersky Embedded Systems Security durante o ciclo de vida do aplicativo (consulte a página sobre o ciclo de vida do aplicativo). Antes de entrar em contato com o Suporte Técnico, leia as regras de suporte.

Você pode entrar em contato com o Suporte Técnico das seguintes formas:

- Ao visitar o site do suporte Técnico
- Enviando uma solicitação ao Suporte Técnico do Kaspersky através 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 detalhes sobre o Kaspersky CompanyAccount, visite o site de Suporte Técnico.

Oferecendo informações de diagnóstico estendidas aos especialistas do Suporte Técnico

Para obter suporte e solução de problemas de aplicativos mais eficazes, os especialistas do Suporte Técnico podem solicitar a alteração temporária das configurações do aplicativo para que seja possível depurá-lo durante o diagnóstico. Esse procedimento talvez exija o seguinte:

- Ativar a funcionalidade que processa e armazena as informações de diagnóstico ampliadas.
- Ajuste fino das configurações dos componentes individuais do software que não estão disponíveis por meio dos elementos padrão da interface do usuário.
- Alterar as configurações de armazenamento e transmissão de informações de diagnóstico que foram processadas.
- Configurar a intercepção e registro de tráfego de rede.

Todas as informações necessárias para a execução das ações listadas (descrição da sequência de etapas, configurações alteráveis, arquivos de configuração, scripts, recursos adicionais de linha de comando, módulos de depuração, utilitários especializados etc.), além da composição dos dados analisados com a finalidade de depuração, serão anunciadas pelos especialistas do Suporte Técnico. As informações de diagnóstico avançadas são salvas no computador do usuário. A transferência automática dos dados armazenados para a Kaspersky não é executada.

Após você reportar um problema aos especialistas de Suporte Técnico, eles poderão solicitar que você crie um relatório com informações sobre a operação do Kaspersky Embedded Systems Security e que o envie ao Suporte Técnico. Os especialistas do Suporte Técnico da Kaspersky poderão solicitar a criação de um arquivo de rastreamento e o envio de um arquivo de despejo de memória.

Após analisar os dados enviados, os especialistas do Suporte Técnico podem criar um script AVZ e enviá-lo para você. Com scripts AVZ, é possível analisar os processos ativos quanto à existência de ameaças, verificar o computador para detectar ameaças, desinfectar ou excluir arquivos infectados e criar relatórios de verificação do sistema.

As ações indicadas acima só podem ser executadas sob a orientação dos especialistas do Suporte Técnico e de acordo com as instruções recebidas. A modificação das configurações do aplicativo sem a devida assistência e de maneira não descrita na documentação do aplicativo ou de maneira não indicada pelas recomendações dos especialistas do Suporte Técnico poderá causar lentidão e funcionamento incorreto do sistema operacional, diminuição do nível de proteção do computador, além de violação de disponibilidade e integridade das informações processadas.

Rastreamento de funcionamento do aplicativo

O *rastreamento do aplicativo* é o registro detalhado de ações executadas pelo aplicativo e das mensagens sobre os eventos ocorridos durante a operação do aplicativo. Durante o processo de rastreamento, o aplicativo cria um conjunto de arquivos com dados sobre a operação de diferentes componentes do aplicativo.

Os arquivos de rastreamento permitem rastrear o processo de execução de comandos do aplicativo, passo a passo, e determinar a etapa da operação do aplicativo em que o erro ocorre.

Os arquivos de rastreamento são armazenados no computador enquanto o aplicativo estiver em uso, e excluídos permanentemente quando o aplicativo for removido. Também é possível excluir os arquivos de rastreamento manualmente. Para fazer isso, é preciso desativar o rastreamento e interromper o aplicativo.

Os arquivos de rastreamento salvos podem conter dados confidenciais. Para controlar o acesso aos dados, será necessário garantir independentemente a segurança dos arquivos de rastreamento.

Por padrão, os arquivos de rastreamento, exceto os arquivos de rastreamento do Agente de Autenticação, são armazenados na pasta: %ProgramData%\Kaspersky Lab\KESS.4.0\Traces.

Os arquivos de rastreamento são nomeados da seguinte forma: KESS<4.0_dateXX.XX_timeXX.XX_pidXXX.><tipo de arquivo de rastreamento>.log.

Você pode visualizar os dados salvos em arquivos de rastreamento.

Todos os arquivos de rastreamento contêm os seguintes dados comuns:

- Hora do evento
- Número do thread de execução

  O arquivo de rastreamento do Agente de Autenticação não contém essas informações.

- Componente do aplicativo que causou o evento
- Grau de gravidade do evento (evento informativo, aviso, evento crítico, erro)
- Uma descrição do evento envolvendo a execução de comando por parte de um componente do aplicativo e o resultado da execução desse comando.

O Kaspersky Embedded Systems Security salva as senhas de usuário em um arquivo de rastreamento somente no formulário criptografado.

Como ativar e configurar o rastreamento do aplicativo no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados**.
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 de propriedades da política, acesse a seção **Diagnóstico de mau funcionamento**.
6. No bloco **Configurações de solução de problemas**, clique no botão **Configurações**.

   A janela **Configurações de solução de problemas** é exibida na guia **Configurações de rastreamento do aplicativo**.
7. Marque a caixa de seleção **Ativar rastreamento**.
8. No campo **Pasta para rastreamento de arquivos**, especifique o caminho absoluto para uma pasta local onde o Kaspersky Embedded Systems Security 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.
9. Na lista suspensa **Nível de detalhes**, selecione o nível de detalhes das informações de depuração:

   - **Crítico** significa que o arquivo de rastreamento salva apenas as mensagens referentes aos erros fatais.
   - **Diagnóstico** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros e avisos.
   - **Importante** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros, avisos e informações adicionais.
   - **Normal** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros e avisos, além das informações sobre a operação normal do aplicativo (padrão).
   - **Detalhado** significa que o arquivo de rastreamento salva todas as informações referentes à operação do aplicativo.

   Um representante do Suporte Técnico determina o nível de detalhe necessário para solucionar qualquer problema que venha a ocorrer.
10. O nível de detalhes padrão é configurado como **Normal**.

11. 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 100 MB.

12. 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.**

13. 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.

14. Salvar alterações.

15. Reinicie o Kaspersky Embedded Systems Security.

Para interromper o rastreamento do aplicativo:

Nas propriedades da política, na janela **Configurações de solução de problemas**, na guia **Configurações de rastreamento do aplicativo**, desmarque a caixa de seleção **Ativar rastreamento.**

Como ativar e configurar o rastreamento do aplicativo no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o node **Kaspersky Embedded Systems Security** e execute uma das seguintes ações:

   - Clique no link **Propriedades do aplicativo** no painel de resultados do node.
   - Selecione **Propriedades do aplicativo** no menu de contexto do node.

   A janela **Propriedades do aplicativo** é aberta.

2. Selecione a guia **Diagnóstico de mau funcionamento.**

3. No bloco **Configurações de solução de problemas**, clique no botão **Configurações.**

   A janela **Configurações de solução de problemas** é aberta.

4. Selecione a guia configurações de rastreamento:

   - **Configurações de rastreamento do aplicativo.** O Kaspersky Embedded Systems Security inicia o rastreamento do aplicativo.
   - **Configurações de rastreamento do Console do Aplicativo.** Caso o Console do Aplicativo e o Kaspersky Embedded Systems Security estejam instalados em computadores diferentes, será possível iniciar o rastreamento somente para o Console do Aplicativo.

5. Marque a caixa de seleção **Ativar rastreamento**.

   O campo **Pasta para rastreamento de arquivos** contém o caminho completo para a pasta local na qual o Kaspersky Embedded Systems Security salva os arquivos de rastreamento por padrão. É possível especificar outro caminho.

6. Na lista suspensa **Nível de detalhes**, selecione o nível de detalhes das informações de depuração:

   - **Crítico** significa que o arquivo de rastreamento salva apenas as mensagens referentes aos erros fatais.
   - **Diagnóstico** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros e avisos.
   - **Importante** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros, avisos e informações adicionais.
   - **Normal** significa que o arquivo de rastreamento salva as mensagens referentes a todos os erros e avisos, além das informações sobre a operação normal do aplicativo (padrão).
   - **Detalhado** significa que o arquivo de rastreamento salva todas as informações referentes à operação do aplicativo.

   Um representante do Suporte Técnico determina o nível de detalhe necessário para solucionar qualquer problema que venha a ocorrer.

   O nível de detalhes padrão é configurado como **Normal**.

7. 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 100 MB.

8. 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**.

9. 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.

10. Salvar alterações.

11. Reinicie o Kaspersky Embedded Systems Security.

Para interromper o rastreamento do aplicativo:

Na janela de propriedades do aplicativo **Configurações de solução de problemas**, na guia **Configurações de rastreamento do aplicativo**, desmarque a caixa de seleção **Ativar rastreamento**.

Como ativar e configurar o rastreamento do aplicativo no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Diagnóstico de mau funcionamento**.
5. No bloco **Configurações de solução de problemas**, marque a caixa de seleção **Ativar rastreamento do aplicativo**.
6. No campo, especifique o caminho completo para uma pasta local onde o Kaspersky Embedded Systems Security 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.
7. Na lista suspensa **Nível**, selecione o nível de detalhes das informações de depuração.
8. 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 100 MB.
9. 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**.
10. 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.
11. Salvar alterações.
12. Reinicie o Kaspersky Embedded Systems Security.

Para interromper o rastreamento do aplicativo:

Nas propriedades da política que está sendo configurada, na seção **Diagnóstico de mau funcionamento**, desmarque a caixa de seleção **Ativar rastreamento do aplicativo**.

[Como ativar e configurar o rastreamento do aplicativo na Interface Compacta de Diagnóstico]

Como ativar e configurar o rastreamento do aplicativo pela linha de comando

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.
2. Usando o comando cd, navegue até a pasta onde o arquivo kavshell.exe está localizado.

   Por exemplo, cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0
3. Execute o seguinte comando:

   KAVSHELL TRACE /ON|/OFF /F:<pasta para armazenar arquivos de rastreamento> [/LVL:debug|info|warning|error|critical] [/S:<tamanho máximo do arquivo de rastreamento em megabytes>] [/R:<número máximo de arquivos de rastreamento antes de substituí-los por novos>]

Registro dos despejos de memória

Um arquivo de despejo de memória contém todas as informações sobre a memória de trabalho dos processos do Kaspersky Embedded Systems Security no momento em que o aplicativo falhou.

Os arquivos de despejo de memória são armazenados no computador enquanto o aplicativo estiver em uso, e excluídos permanentemente quando o aplicativo for removido.

Os arquivos de despejo salvos podem conter dados confidenciais. Para controlar o acesso aos dados, é necessário garantir independentemente a segurança dos arquivos de despejo de memória.

Por padrão, os arquivos de despejos de memória são armazenados na seguinte pasta: %ProgramData%\Kaspersky Lab\KESS.4.0\Traces.

Como ativar ou desativar a gravação do despejo de memória no Console de Administração do Kaspersky Security Center

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o node **Dispositivos gerenciados**.
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 de propriedades da política, acesse a seção **Diagnóstico de mau funcionamento**.

6. No bloco **Configurações de solução de problemas**, clique no botão **Configurações**.

   A janela **Configurações de solução de problemas** é exibida na guia **Configurações de rastreamento do aplicativo**.

7. Selecione a guia **Configurações de despejo do aplicativo**.

8. Marque ou desmarque a caixa de seleção **Criar arquivo de despejo** para ativar ou desativar o despejo de memória em caso de funcionamento incorreto.

9. Caso seja necessário, no campo **Pasta de arquivos de despejo**, insira o caminho completo da pasta local onde o Kaspersky Embedded Systems Security salvará os arquivos de despejo de memória.

   > 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.

10. Salvar alterações.

Como ativar ou desativar a gravação do despejo de memória no Console do Aplicativo

1. Na árvore do Console do Aplicativo, selecione o node **Kaspersky Embedded Systems Security** e execute uma das seguintes ações:

   - Clique no link **Propriedades do aplicativo** no painel de resultados do node.
   - Selecione **Propriedades do aplicativo** no menu de contexto do node.

   A janela **Propriedades do aplicativo** é aberta.

2. Selecione a guia **Diagnóstico de mau funcionamento**.

3. No bloco **Configurações de solução de problemas**, clique no botão **Configurações**.

   A janela **Configurações de solução de problemas** é aberta.

4. Selecione a guia configurações de despejo:

   - **Configurações de despejo do aplicativo**. O Kaspersky Embedded Systems Security registra todos os despejos do aplicativo.
   - **Configurações de despejo do Console do Aplicativo**. Caso o Console do Aplicativo e o Kaspersky Embedded Systems Security estejam instalados em computadores diferentes, será possível registrar despejos somente para o Console do Aplicativo.

5. Marque ou desmarque a caixa de seleção **Criar arquivo de despejo** para ativar ou desativar o despejo de memória em caso de funcionamento incorreto.

   Por padrão, os arquivos de despejos de memória são armazenados na seguinte pasta: %ProgramData%\Kaspersky Lab\KESS.4.0\Traces. É possível especificar outro caminho.

6. Salvar alterações.

Como ativar ou desativar a gravação do despejo de memória no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Ativos (dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do Kaspersky Embedded Systems Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Diagnóstico de mau funcionamento**.
5. Em **Configurações do arquivo de despejo**, marque ou desmarque a caixa de seleção **Criar arquivo de despejo** para ativar ou desativar o despejo de memória em caso de funcionamento incorreto.
6. Caso necessário, especifique o caminho completo para uma pasta local onde o Kaspersky Embedded Systems Security salvará os arquivos de despejo de memória.

   > 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.
7. Salvar alterações.

Também é possível ativar ou desativar a gravação do despejo de memória na Interface Compacta de Diagnóstico.

Fontes de informação sobre o Kaspersky Embedded Systems Security

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

- Acesse a página do Kaspersky Embedded Systems Security no site da Kaspersky
- Página do Kaspersky Embedded Systems Security no site do Suporte Técnico (Base de dados de conhecimento)
- Ajuda online
- Discussão sobre os aplicativos da Kaspersky no fórum

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 no site da Kaspersky

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

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

Página do Kaspersky Embedded Systems Security 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 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, mas também com outros aplicativos da Kaspersky. Os artigos da Base de Dados de Conhecimento podem também incluir notícias sobre o Suporte Técnico.

Ajuda online do Kaspersky Embedded Systems Security

A ajuda online contém as informações de configuração e uso do Kaspersky Embedded Systems Security.

Discussão sobre os aplicativos da Kaspersky no fórum

Se sua pergunta não exigir uma resposta urgente, você pode falar sobre ela com os especialistas da Kaspersky e com outros usuários no nosso Fórum.

No Fórum, é possível ver os tópicos existentes, postar seus próprios comentários e criar novos tópicos de discussão.

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 compactado

Um ou vários arquivos foram compactados em um único arquivo compactado. Um aplicativo especializado chamou um arquivador que é necessário para compactar e descompactar dados.

Arquivo infectável

Um arquivo que, devido a sua estrutura ou ao seu formato, pode ser usado por invasores como um "contêiner" para armazenar e difundir um código malicioso. Normalmente, são arquivos executáveis com extensões como .com, .exe e .dll. Existe um risco bastante alto de intrusão de código malicioso nesses arquivos.

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

Os bancos de dados contêm informações sobre ameaças à segurança do computador conhecidas da Kaspersky na data de publicação do banco de dados de antivírus. As assinaturas de banco de dados de antivírus ajudam a detectar código malicioso em objetos verificados. Os bancos de dados do antivírus são criados pelos peritos da Kaspersky e atualizados a cada hora.

Chave ativa

Chave que está atualmente em uso pelo aplicativo.

Configurações de tarefa

Configurações específicas do aplicativo para cada tipo de tarefa.

Desinfecção

Um método de processar objetos infectados que resulta em recuperação total ou parcial de 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.
- Mensagem informativa.

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 nas máscaras de arquivo são * e ? (em que * representa qualquer número de caracteres e ? representa qualquer caractere único).

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 como tarefas, por exemplo: Proteção de Arquivos em Tempo Real, Verificação Completa 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, localizado na pasta de instalação do aplicativo.

Avisos de marcas registradas

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

Apache é uma marca registrada ou uma marca comercial da Apache Software Foundation.

Citrix, XenApp e XenDesktop são marcas registradas ou marcas comerciais do Cloud Software Group, Inc., e/ou de suas subsidiárias nos Estados Unidos e/ou em outros países.

CVE é uma marca registrada da The MITRE Corporation.

Dell Technologies, Dell, Dell Compellent e outras marcas comerciais são marcas comerciais da Dell Inc. ou de suas subsidiárias.

EMC, Celerra, Isilon, OneFS e VNX são marcas registradas ou marcas comerciais da EMC Corporation nos Estados Unidos e/ou em outros países.

Hitachi é uma marca registrada da Hitachi, Ltd.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e em outros países.

Microsoft, Active Directory, Internet Explorer, Excel, Hyper-V, JScript, MultiPoint, Outlook, PowerShell, Windows, Windows Server e Windows Vista são marcas registradas do grupo de empresas Microsoft.

NetApp e Data ONTAP são marcas comerciais ou marcas registradas da NetApp, Inc. nos Estados Unidos e/ou em outros países.

Oracle é uma marca registrada da Oracle Corporation e/ou suas afiliadas.

UNIX é uma marca registrada nos Estados Unidos e em outros países, licenciada exclusivamente pela X/Open Company Limited.

Apêndices

Esta seção contém informações que complementam o corpo do documento.

Extensões de arquivo para verificação rápida

com – arquivo executável de um aplicativo de até 64 KB

exe – arquivo executável ou arquivo autoextraível

sys – arquivo do sistema Microsoft Windows

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

bin – arquivo binário

bat – arquivo em lote

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

dpl – biblioteca Borland Delphi compactada

dll – biblioteca de link dinâmica

scr – tela de início do Microsoft Windows

cpl – módulo do painel de controle do Microsoft Windows

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

tsp – programa que executa em modo de tempo parcial

drv – driver de dispositivo

vxd – driver de dispositivo virtual do Microsoft Windows

pif – arquivo de informações de programa

lnk – arquivo de link do Microsoft Windows

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

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

cla – classe de Java

vbs – script do Visual Basic®

vbe – extensão de vídeo de BIOS

js, jse – texto de fonte de JavaScript

htm – documento de hipertexto

htt – cabeçalho de hipertexto do Microsoft Windows

hta – programa de hipertexto do Microsoft Internet Explorer®

asp – script de Páginas do Servidor Ativo

chm – arquivo HTML compilado

pht – arquivo HTML com scripts PHP integrados

php – script integrado em arquivos HTML

wsh – arquivo do Microsoft Windows Script Host

wsf – script do Microsoft Windows

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

hlp – arquivo Win Help

msg – mensagem de e-mail do Microsoft Mail

plg – mensagem de e-mail

mbx – mensagem de e-mail salva do Microsoft Outlook Express

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

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

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

rtf – documento de Formato Rich Text

shs – fragmento do manipulador de objeto do Windows Shell Scrap

dwg – banco de dados de desenho do AutoCAD®

msi – pacote do Microsoft Windows Installer

otm – projeto VBA para Microsoft Office Outlook

pdf – documento do Adobe Acrobat

swf – objeto de pacote do Shockwave® Flash

jpg, jpeg – formato gráfico de imagem compactada

emf – arquivo de formato de Metarquivo Aprimorado;

ico – arquivo de ícone de objeto

ov? – Arquivos executáveis do Microsoft Office Word

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

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

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

sldx – um slide do Microsoft PowerPoint 2007

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

thmx – um tema do Microsoft Office 2007

Contas de usuário em regras de componentes de aplicativos

Para configurar alguns componentes do aplicativo, é necessário adicionar regras especiais em que você pode selecionar os usuários aos quais o aplicativo aplicará a regra.

As regras devem ser adicionadas para configurar os seguintes componentes do aplicativo:

- Controle de Inicialização de Aplicativos
- Controle de Dispositivos

- Detecção de Comportamento.
- Monitor de integridade do sistema

É possível adicionar usuários das seguintes maneiras:

- Selecionar pelo Active Directory (recomendado)
- Selecionar pela lista de usuários do Kaspersky Security Center
- Adicionar manualmente

A Kaspersky recomenda usar contas de usuário locais somente em casos especiais quando não for possível usar contas de usuário de domínio. Para obter detalhes sobre os riscos de segurança quanto ao uso de contas locais, consulte a Base de Dados de Conhecimento da Microsoft. O usuário assume total responsabilidade pela segurança de um computador caso as contas de usuário locais sejam usadas. Em particular, isso inclui a responsabilidade de controlar e restringir o acesso às configurações do aplicativo.

O aplicativo usa o SID (Identificador de Segurança) do usuário para identificar os usuários. Ao usar as contas de usuário do Active Directory ou da lista de usuários do Kaspersky Security Center, o aplicativo determina o SID no Servidor de Administração. Isso significa que o aplicativo não coloca carga extra no computador para identificar um usuário. Caso tenha adicionado mais de 1.000 contas de usuário locais a uma regra de aplicativo, os aplicativos entrarão em contato com o controlador de domínio para identificar o usuário. Isso significa que a carga no computador é aumentada. Para otimizar o impacto no desempenho do computador, recomendamos usar contas de usuário do Active Directory ou da lista de usuários do Kaspersky Security Center.

O Kaspersky Embedded Systems Security é compatível com contas de usuário e grupo integrados (por exemplo, o grupo "Todos") nas regras. Devido às especificidades da detecção do SID do usuário, o aplicativo permite o uso de contas integradas adicionadas somente do Active Directory ou da lista de usuários do Kaspersky Security Center. As regras nas quais a conta integrada é adicionada manualmente não funcionam.